IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 November 2025, accepted 30 November 2025, date of publication 8 December 2025,
date of current version 19 December 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3641180

RESEARCH ARTICLE

Cybersecurity Ethical Aspects (CEA)

JAFAR ABABNEH[1], (Member, IEEE), MAJED MOHAMMED ALNEMARI[2], HANI ATTAR[3], HANI A. ALGHAMDI[2], MUATH AL-SHAWAHEEN[2], BALQIES SAQARAT[2], LAILA ABU ROMMAN[2], AND MUSAB IQTAIT[4]

[1]Faculty of Information Technology, Zarqa University, Zarqa 13110, Jordan
[2]Faculty of Engineering, Mutah University, Karak 61710, Jordan
[3]Faculty of Engineering, Zarqa University, Zarqa 13110, Jordan
[4]Department of Data Science and Artificial Intelligence, Faculty of Information Technology, Zarqa University, Zarqa 13110, Jordan

Corresponding author: Jafar Ababneh (jababneh@zu.edu.jo)

ABSTRACT In the contemporary digital landscape, cybersecurity must be regarded not merely as a technological matter but as an issue with profound ethical implications. The article analyzes the various ethical concerns inherent in modern cybersecurity advancements, encompassing data privacy, mass surveillance, algorithmic discrimination, corporate equality, and cyber warfare. The study achieves its aim through an analytical examination of scholarly literature and by presenting case studies, including Facebook-Cambridge Analytica, the Stuxnet cyber weapon and more, to demonstrate how ethical lapses erode confidence, civil rights, and democratic principles. The study presents a more extensive valid tiered ethical cybersecurity model (TECM) than prior research due to its integrative perspective that connects normative ethical theories with practical regulatory methods, suggesting a multi-domain approach that has not been statistically assessed in earlier studies. The study clarifies the varying legal status of international guidelines, the mechanisms of consent, and the instruction of ethical principles to cybersecurity professionals, which will increase the applicability of recommendations across various legal and cultural contexts. The paper emphasizes the necessity of safeguarding the digital domain grounded in equity, responsibility, and human dignity. The findings underscore the necessity for practitioners and policymakers to integrate accountability, transparency, fairness, and proportionality at all stages of cybersecurity planning and implementation. The tiered approach can inform regulations, corporate governance principles, and incident response protocols. The paper provides pragmatic guidance for non-academic audiences on mitigating AI bias in cybersecurity solutions, ensuring corporate accountability in data management, and balancing privacy with national security.

INDEX TERMS Algorithmic bias, artificial intelligence, corporate responsibility, cybersecurity ethics, cyberwarfare, data privacy, ethical governance, informed consent, surveillance.

I. INTRODUCTION

With the swift progression of technology, cybersecurity has come to encompass a broad range of legal, economic, political, and particularly ethical issues. The Internet of Things, cloud services, and artificial intelligence have augmented both the volume of data and the velocity of its dissemination over networks. The proliferation of connected devices and interconnectivity creates chances for cyber risks, such as data breaches, identity theft, cyber espionage, and ransomware assaults. Thus, ethical issues are essential to the formulation and management of any positive cybersecurity strategy.

Ethical dilemmas in cybersecurity are crucial to important discussions. Who possesses data? Who is accountable if an online system malfunctions? What measures can corporations and governments implement to safeguard security while preserving privacy? The significance of these questions is escalating because of the extensive collection, storage, and processing of personal and sensitive data by both governmental and commercial organizations. Incidents such as the Equifax and Facebook-Cambridge Analytica hacks have exposed both technical deficiencies and

The associate editor coordinating the review of this manuscript and approving it for publication was Cong Pu.

© 2025 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License.
For more information, see https://creativecommons.org/licenses/by/4.0/

ethical failures concerning openness, consent, and responsibility [1], [2].

The ethical approach to cybersecurity is increasingly recognized as a fundamental component of sustainable and responsible cybersecurity practices. The necessity for ethical judgments is no longer optional, as every decision inside the technical realm may influence the choice between life and death, with computers increasingly capable of making high-stakes decisions. The decision-making systems utilizing AI, along with user behavior tracking and predictive analysis, increasingly present complex ethical compromises in their execution. Such lapses represent not only technology deficiencies but also ethical failings that can undermine democracy, liberty, and social trust. Consequently, integrating ethical principles such as openness, accountability, fairness, and respect for autonomy into cybersecurity systems is crucial for preserving integrity in digital contexts [3].

Multilateral institutions have recently acknowledged the necessity for accountable governance in cyberspace. The European Union General Data Protection Regulation (GDPR) emphasizes both legal compliance and the ethical foundations of data protection, encompassing fairness and data reduction. Similarly, ethical principles that should accompany technology implementation are outlined in the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data released by the Organization for Economic Co-operation and Development (OECD). The texts indicate a growing consensus on the necessity of ethical cybersecurity that takes into account legal obligations and societal impacts.

In numerous developing and transitional nations, the cybersecurity infrastructure is being established more rapidly than the ethical standards and legal frameworks that should govern it. The mismatch may result in significant power bias, unmonitored observation, data exploitation, and biased algorithms. In the absence of a robust ethical framework, digital transformation in many situations may exacerbate inequality, marginalization, or political oppression. Therefore, ensuring that ethical considerations guide digital policy-making not only in technologically advanced nations but also in emerging ones is very necessary [4].

To bridge the gap between theoretical understanding of ethical issues and their practical implementation in cybersecurity, researchers and organizations have created various conceptual frameworks that delineate the ethical dimensions of cybersecurity. These frameworks facilitate the implementation of ethical values across several levels of digital architecture and decision-making processes inside an organization. Integrating a complete structural ethical framework in cybersecurity would improve risk management, governance transparency, and the advancement of ethical technologies [5].

The research indicates that cybersecurity necessitates the safeguarding of individuals' rights, freedoms, and equitable treatment in the digital realm.

Cybersecurity ethics is founded on the principles of societal welfare and their application within cyberspace. These ethical frameworks assist leaders in making diverse value judgments regarding the disclosure of unknown vulnerabilities, evaluating the ethics of penetration testing, and delineating the obligations of developers of artificial intelligence systems that generate unforeseen risks. The escalating complexity of cybersecurity threats necessitates the integration of robust ethical concepts into all cyberspace policies and actions.

Cybersecurity ethics encompasses various concerns, including the safeguarding of private information, the responsible development and management of data-driven technology, and the adherence to international cybersecurity standards. Addressing these issues necessitates the formulation of both comprehensive legal and technical strategies, alongside an elevated ethical consciousness across all relevant domains. The study examines the various ethical aspects of cybersecurity, along with the challenges, frameworks, and implications related to each.

Despite advancements in cybersecurity technologies, the integration of ethical concepts at the technical, organizational, and policy levels remains significantly constrained. A primary challenge identified is the lack of a unified standard for ethical conduct, resulting in varying responses based on the specific jurisdiction involved. Furthermore, the significant opacity of their activities, particularly those related to AI, obstructs transparency and undermines trust in these systems. Moreover, the majority of organizations do not regard ethical violations as a proactive issue; rather, they react to them, typically driven by economic considerations or insufficient ethical awareness. Particularly in international contexts where regulatory discrepancies are most pronounced, these deficiencies hinder the establishment of equitable and authentic cybersecurity environments.

Figure 1 illustrates the systematic integration of ethical standards into the five fundamental components of the NIST cybersecurity framework: identify, protect, detect, respond, and recover besides that, Table 1 delineates particular ethical evaluations and demonstrates their alignment with NIST operations, offering a pragmatic framework for execution in automated decision-making systems [6] and [7].

All functions are complemented by corresponding ethical values derived from the information ethics proposed by Floridi and many texts on digital ethics [8]. Cyber risk definitions should adhere to the principle of privacy, ensuring that risk assessments do not violate individual rights. Protective mechanisms are designed to avert injury, especially those resulting from negligence, bias, or excess.

The detection systems must promote a sense of independence by being explicable, transparent, and aware of user agency. Responses to cyber incidents must promote justice through proportional measures, due process, and transparency. Finally, recovery activities should promote the application of justice, ensuring that victims receive assistance and that system restoration occurs in a fair and inclusive manner, where correlation of ethical ideals with cybersecurity

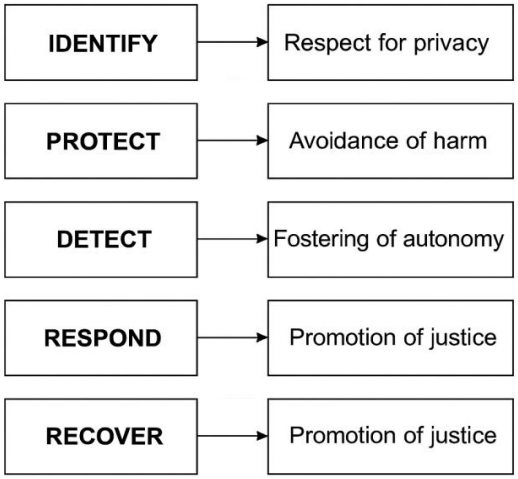


FIGURE 1. Ethical integration within the NIST cybersecurity framework.

operations illustrates that ethical considerations are not solely theoretical but function as pragmatic guidelines designed to foster trust, responsibility, and enduring resilience across time.

A. LIMITATIONS AND CHALLENGES

While the suggested study positively influences a more integrated approach to cybersecurity ethics, many limitations warrant acknowledgment. The TECM model validation study predominantly utilizes a participant pool from three stakeholder groups (faculty, students, and industry professionals), neglecting the full spectrum of individuals involved in cybersecurity practice and employing only three country categories, thereby limiting the generalizability of cross-cultural comparisons.

Secondly, Reliance on self-reporting Likert-scale assessments may result in biases, such as social desirability and answer consistency effects. Participants may amplify their ethical consciousness or sense of obligation to align with perceived expectations.

Third, ethical attitudes and legal frameworks vary by country, complicating the generalization of advice worldwide.

Lastly, the swift advancements in cybersecurity technologies may complicate the maintenance of existing ethical frameworks, including those related to generative AI and quantum computing.

B. CONTRIBUTIONS

The paper offers several notable contributions to the field of cybersecurity ethics:

- This study methodically combines literature ethical theories; AI ethics, cybersecurity and governance with actual cybersecurity incidents to offer practical insights for ethically informed decision-making and policy formulation.
- It examines a substantial body of recently published material, integrating both theoretical and practice-based perspectives to illustrate contemporary ethical dilemmas.
- Its offerings Comparative analysis of fifteen significant cybersecurity cases uncover persistent themes and emerging ethical dilemmas.
- It presents a validate model (TECM) in the form of a tiered network that offers recommendations for the ethical integration of cybersecurity processes across technological, organizational, and policy dimensions.
- The study highlights significant regulatory flaws currently in existence and points out that there must be a worldwide agreement and monitoring mechanism.
- It introduces the Tiered Ethics Cybersecurity Model (TECM), a systematic five-tier ethical governance paradigm comprising Foundational Ethics, Applied Ethics, and Adaptive Ethics. The TECM distinguishes itself from other principle-based models by deconstructing ethical reasoning into layers that link normative principles with their practical application and subsequent translation into policy.
- The TECM advances the discourse on responsible AI and digital governance by linking ethical concepts to adaptable policy frameworks. Incorporating an adaptive policy layer enables institutions to dynamically synchronize their ethical commitments with evolving

TABLE 1. Mapping of ethical checks to NIST CSF functions.

NIST CSF Function	Subcategory	Ethical Check	Worked Example
Identify	ID.AM (asset management)	AI asset & data ethics inventory	Maintain a register of models and datasets, and identify sensitive aspects.
Identify	ID.GV (governance)	Ethical governance framework	Policies for AI fairness, transparency, accountability
Protect	PR.AC (access control)	Access control for sensitive data	Bound access to personal data for AI training
Protect	PR.IP(data integrity)	Data integrity validation	Authenticate dataset consistency and absence of manipulative features
Detect	DE.CM (continuously monitor)	Bias/anomaly detection	Monitor ML outputs for fairness abuses
Detect	DE.DP (detection Processes)	Continuous ethical monitoring	Track AI decision patterns over time
Respond	RS.RP (response planning)	Human-in-the-loop review	Trigger review workflow for biased AI outputs
Respond	RS.MI(mitigation)	Corrective action enforcement	Suspend or modify decisions when ethical anomalies occur
Recover	RC.IM (Improvement)	Post-incident model retraining	Retrain AI models with verified unbiased datasets
Recover	RC.CO (Communications)	Transparency reporting	Publish incident reports to maintain trust

technological, legal, and social circumstances to ensure that judgments are rendered transparently, responsibly, and sustainably.
- Mapping ethical checks onto the NIST CSF functions in both narrative and tabular form, which is a useful operationalization for practitioners.
- Lastly, the paper is beneficial for practitioners and policymakers to identify tools that promote trust, transparency, and resilience in cybersecurity, along with a detailed analysis of each cybersecurity function in relation to ethical ideals.

The article is structured as follows. Section II provides a comprehensive review of the existing literature on ethical theories and the practical issues associated with contemporary activities in the cybersecurity domain. Section III examines significant case studies to illustrate ethical dilemmas practically. The IV section validate the proposed model, elucidates the principal findings and their subsequent implications for policy and practice by section V, section VI delineates the recommendations derived from the analysis and concludes with a summary of key insights and prospective research directions represented in section VII.

II. LITERATURE REVIEW

A literature review was performed utilizing IEEE Xplore, Scopus, Web of Science, ACM Digital Library, and Google Scholar. The search employed Boolean keyword combinations such as ''cybersecurity ethics,'' ''ethical cybersecurity,'' ''algorithmic bias + cyber threat detection.'' ''AI fairness,'' and ''privacy-aware intrusion detection,''.

The research examines AI-driven cybersecurity and ethical governance from 2015 to 2025. The studies encompassed cybersecurity and machine learning-based intrusion detection systems that were Peer-reviewed journals, conference papers, technical reports on cybersecurity or AI ethics and specifically addressed ethical, justice, or regulatory concerns. Opinion articles lacking evidence, non-English publications, and duplicate indexed entries were excluded. 283 records identified, only 106 were deemed suitable after title and abstract screening, and 36 met all eligibility criteria for inclusion in the final evaluation.

Table 2 chronologically presents a comprehensive summary by outlining the methodology, strengths, weaknesses, and limitations of each study to promote scientific transparency and reproducibility.

Theoretical security development pervades academic literature, despite the increasing prevalence of cybercrime in society and the concomitant reliance on digital technology. Academics have addressed ethical and cybersecurity challenges from several perspectives, including data privacy, surveillance, algorithmic responsibility, and moral duties of both nation-states and non-governmental entities.

Abd Rahim et al. [9] examine evaluation methodologies for cybersecurity awareness, including organizational and behavioral strategies, therefor the study enhances awareness measurement frameworks but offers minimal insights into long-term impact.

Kushwaha et al. [10] emphasize the imperative of implementing stringent information security measures and a clearly defined legal framework to safeguard sensitive consumer data from fraud and misuse, drawing attention to the importance of regulatory policies in upholding ethical standards and enhancing consumer confidence in online transactions.

Kumar et al. [11] concurrently examined the ethical dimensions of artificial intelligence, emphasizing the perils associated with algorithmic inaccuracy, opacity, and the potential for AI-enabled surveillance to undermine individual freedom and privacy, unless adequate security measures are implemented.

Kavallieros et al. [12] examined the legal and ethical challenges in cybercrime detection, emphasizing the complexities of ensuring due process. They stressed the need to balance public interest with civil liberties and advocated for the establishment of additional procedural norms and enhanced cross-jurisdictional collaboration with international partners.

Wilk [13] analyzes cybersecurity education and legal frameworks, emphasizing the significance of ethical literacy for professionals. The work offers foundational information but is limited by its emphasis on educational situations and fails to evaluate the practical influence on professional behavior.

Mittelstadt [14] presents a narrative overview addressing ethical dilemmas in the health-related Internet of Things, including privacy, autonomy, and data governance. The study posits ethical design as essential to health technology innovation, although it lacks practical implementation indicators.

Yaghmaei [15] explores the ethical discourse surrounding cybersecurity policy, advocating for responsibility, accountability, and inclusivity in governance. The paper contributes valuable normative insights but remains conceptual without empirical substantiation.

Jalali and Kaiser [16] present a systematic review of cybersecurity in hospitals, framing security as an organizational and cultural issue rather than purely technical. While conceptually rich, it lacks empirical depth and generalizability beyond healthcare contexts.

Švábenský et al. [17] conduct a systematic literature review of cybersecurity education research presented at major ACM conferences, revealing trends in pedagogy, assessment, and engagement. The analysis is broad but limited by reliance on a narrow publication set.

Macnish and van der Ham [18] conducted a comprehensive analysis of the ethical components in cybersecurity research, highlighting the importance of researcher accountability and professional duty. Their analytical methodology provides conceptual clarity but lacks quantitative confirmation, highlighting the necessity for empirically based ethics metrics in cybersecurity operations.

Pattison [19] examined the ethical limits of private cybersecurity measures from a normative ethics perspective, differentiating between defensive and aggressive cyber acts.

The study provides significant philosophical insight; yet, it is context-dependent and necessitates practical models that connect ethical reasoning with corporate cybersecurity governance.

Engster [20] introduced a stakeholder-based, care ethics approach to cybersecurity in business environments, advocating ethical inclusion in decision-making processes. The model effectively bridges social responsibility and cybersecurity management but remains theoretical, highlighting the absence of empirical testing or industry-based application.

Ulven and Wangen [21] conduct a systematic analysis of cybersecurity threats in higher education, pinpointing institutional vulnerabilities and the necessity for governance-oriented mitigation strategies. The review provides a thorough synthesis but is deficient in quantitative risk modeling and cross-sector validation.

Leitão and Karnouskos [22] investigate ethical engineering in industrial cyber-physical systems, highlighting the incorporation of ethical issues into system design. The paper promotes responsible deployment of CPS but is primarily conceptual, with minimal empirical validation in actual industrial settings.

Kozhuharova et al. [23] identified emerging ethical challenges in digital service chains using case-driven qualitative analysis. Their framework delineates moral responsibility among stakeholders yet lacks quantitative assessment, revealing the need for standardized ethics evaluation protocols in complex cybersecurity ecosystems.

Alsharida et al. [24] synthesized behavioral, ethical, and technical dimensions of cybersecurity, emphasizing human factors in ethical vulnerability. The study consolidates multi-perspective insights but fails to propose a structured ethical framework, limiting its direct applicability in cybersecurity policy design.

Flechais and Chalhoub [25] mapped CyBOK knowledge domains to ethical responsibilities, operationalizing professional ethics in cybersecurity practice. Although innovative in linking ethics to standardized body-of-knowledge structures, the study's reliance on expert workshops constrains generalizability beyond the academic context.

Matei and Bertino [26] proposed an educational approach that integrates ethics, systems thinking, and communication into AI-cybersecurity training. The methodology improves the development of ethical competency but is still theoretical, highlighting a deficiency in longitudinal validation and pedagogical evaluation of ethical learning outcomes.

Gupta et al. [27] examined the duality of employing generative AI tools, such as ChatGPT, in cybersecurity, illustrating that these applications can function as both offensive and defensive mechanisms while highlighting the absence of established ethical standards for the domain.

SciSpace [28] compiled 71 influential works in the domain of privacy and security in 2023, illustrating the rapid expansion of ethical and technological literature.

Thirumuruganathan et al. [29] proposed viable techniques for identifying and rectifying sample bias in intrusion detection systems; nonetheless, their approach has notable limitations about its practical implementation in real-world scenarios. Damola and Miracle [30] studied the effects of algorithmic bias in AI-driven threat detection systems and examined methods to mitigate false alarms by diversifying training datasets.

Dasu et al. [31] introduced NeuFair, a dropout-based model for rectifying fairness in neural networks, achieving up to 69 percent improvement; however, its randomization mechanism led to inference instability in certain contexts.

Mahadik et al. [32] have proposed a privacy-preserving intrusion detection framework for Internet of Medical Things (IoMT) systems to improve data security; nevertheless, it is currently constrained by the absence of diverse datasets for testing. Additional remarks pertinent to the subject address algorithmic impartiality in cybersecurity [33], privacy-conscious deep learning systems for intrusion detection [34], ethical AI governance frameworks [35], and the prospective evolution of international data protection legislation prior to 2025 [36].

Ewoh and Vartiainen [37] conducted a systematic review on ethical and sociotechnical vulnerabilities in healthcare cybersecurity systems. Their findings underscore the interplay between privacy ethics and system resilience but are limited to the healthcare domain, constraining broader cross-sector implications.

Alanezi and Al-Azzawi [38] analyzed dual-use ethical dilemmas in AI-powered cyber threat development, emphasizing the moral hazard of autonomous defensive systems. While conceptually robust, the lack of empirical validation highlights the necessity of integrating real-world case evaluation into AI-ethics research.

Mubarak and Aldhmour [39] examined the ethical dimensions of hacking and moral hazard in cyberspace, focusing on data transparency and accountability. Their comparative framework advances understanding of ethical hacker behavior but lacks stakeholder validation, suggesting future mixed-method research on trust and moral risk.

Wheeler [40] outlines anticipated global privacy and cybersecurity regulations for 2025, emphasizing risk-based, ethics-driven frameworks and cross-border accountability. The study highlights the need for transparency and resilience in organizational compliance. Its limitation lies in its largely normative approach, lacking empirical validation across diverse jurisdictions

Kim et al. [41] introduced a payload-aware intrusion detection model utilizing big language models and contrastive learning, demonstrating significant promise in classification performance, but it is computationally intensive.

Berkeley Lab [42] evaluated the geopolitical imbalances in cybersecurity governance and underscored the lack of an international incident contingency.

Mladenov and Galetin [43] provide a rigorous legal–ethical interpretation of encryption as a human right within the jurisprudence of the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU). Their analysis reframes encryption as a cornerstone of digital autonomy and resistance against surveillance. Although comprehensive in legal scope, the study's limitation lies in its jurisdictional confinement, signaling the need for comparative research on encryption ethics beyond the European legal sphere.

Popa Tache and Vâlcu [44] explore the intersection between artificial intelligence governance and corporate legal responsibility, proposing an ethical–legal contract that harmonizes human rights with emerging AI accountability frameworks. The study contributes to the ethical regulation of autonomous corporate actions, yet its conceptual nature and absence of empirical application underline the need for multidisciplinary validation across corporate, legal, and technological contexts.

Algorithmic biases in detection can significantly affect cybersecurity outcomes when systems depend on insufficient or unidimensional data inputs. Ababneh et al. (2024) conducted a study demonstrating the optimization of accuracy using various edge detection algorithms applied to RGB color channels, suggesting that additional channels may mitigate algorithmic blind spots [45].

All these studies reflect the rapid advancement of the profession focused on integrating ethics into cybersecurity technologies and policies. Table 2 chronologically presents a comprehensive summary of their tactics, strengths, shortcomings, and limits and ultimately outlines the contribution of the integrated ethical framework to the current study.

A. ETHICAL FOUNDATIONS OF CYBERSECURITY

A comprehensive grasp of ethical philosophy is crucial for analyzing the ethical dimensions of cybersecurity. Initial discourse on cybersecurity mostly focused on the formulation of technical solutions; however, contemporary study increasingly emphasizes ethical philosophy in light of the escalating concerns presented by increased digitization. The authors propose a novel perspective termed ''information ethics,'' reinterpreting cybersecurity from a defensive approach to a balanced moral obligation towards cybersecurity. They regard data systems, databases, and executing algorithms as having distinct moral significance inside the digital realm which encourages cybersecurity experts to view information not just as a tool for protection but as an ethically significant entity. Consequently, the ethical obligation to maintain informational privacy, autonomy, and dignity motivates the safeguarding of data obtained through the method [3].

Manjikian (2017) [46] proposes a fair war theory framework for evaluating cyber operations. She inquires if nations should be permitted to execute preemptive cyberattacks in the absence of substantial evidence indicating an impending harmful event. The notion of proportionality becomes increasingly important because cyber war actions inevitably damage systems vital to civilian welfare. Manjikian's invocation of traditional military ethics in cyberwarfare underscores the necessity of establishing a consensus on ethical principles to regulate conflicts in cyberspace.

In 2016, Stahl et al. [47] underscore that professionals in IT and cybersecurity have an obligation to integrate ethical issues at every phase of technology development and implementation. The governing authorities have established their own ethical norms to direct the utilization and advancement of digital technology.

They implore engineers to methodically evaluate the ethical dimensions at each phase of software creation and implementation, from inception to deployment which aligns with the growing belief that ethical principles should be integrated into the fundamental design of technology rather than added as an afterthought. The necessity for these ethical foundations is further emphasized by the emergence of new technologies such as AI, biometric surveillance, and the Internet of Things (IoT).

Brey (2012) [48] asserts that emerging technologies develop at a pace surpassing the regulatory frameworks governing their ethical and legal applications, resulting in unmitigated potential harms. The emergence of these gaps subject's cybersecurity experts to significant risks of inadvertent damage or the exacerbation of privacy, autonomy, and equality concerns, Therefore, attaining ethical literacy and a solid philosophical framework is crucial for effective cybersecurity governance.

B. PRIVACY AND SURVEILLANCE ETHICS

Cybersecurity's delicate balance between individual rights and state security remains critical. As digital technologies grow, citizens, scholars, and politicians increasingly divide over public safety surveillance. Privacy and security conflicts are a major issue in ethical cybersecurity. Shoshana Zuboff's ''The Age of Surveillance Capitalism'' (2019) is a landmark study of how internet companies profit from data. Zuboff defines ''surveillance capitalism'' as an economic system that profits from collecting, analyzing, and selling personal data. Most terms of service are unclear and contractual, so users are unaware of how their personal data is collected, used, and sold.

Zuboff [49] claims that information asymmetries prevent consumers from regulating the use of their personal data, making the activity more than a privacy violation and for reducing data exploitation stricter laws were suggested.

Governments implement various forms of comprehensive surveillance into society. Facial recognition, biometrics, predictive analytics, and transnational data sharing are key components of many nations' security efforts to combat terrorism, organized crime, and cybercrime. Lyon warns that such surveillance infrastructures may lead to ''surveillance societies,'' where people are assumed to be dangerous unless they prove otherwise, where advancement often occurs without public supervision or ethical review, eroding civil liberties and surveillance protections in democracies predicated on

TABLE 2. Comparative summary of ethical cybersecurity.

Authors	Year	Approach	Advantages	Disadvantages	Limitation
N. H. Abd Rahim et al[9]	2015	Systematic review of cybersecurity awareness assessment methods	Consolidates behavioral and organizational frameworks	Inconsistent longitudinal approaches	Lacks evaluation of long-term awareness impact
Kushwaha et al. [10]	2016	Legal safeguards in online finance	Promotes user confidence	Implementation complexity	Limited adaptation to evolving fraud
Kumar et al. [11]	2016	Ethical analysis of AI surveillance	Highlights privacy risks	Lacks mitigation strategies	Based on hypothetical scenarios
Kavallieros et al. [12]	2016	Legal-ethical review of cybercrime detection	Supports procedural norms	Balancing civil liberties is difficult	No standardization across jurisdiction
Wilk [13]	2016	Cybersecurity ethics education	Fosters comprehensive professional skills	Dependent on institutional support	Scalability challenges
B. Mittelstadt[14]	2017	Narrative review on ethics in health-related IoT	Integrates privacy, autonomy, and governance into IoT ethics	Conceptual and lacks applied metrics	No empirical validation of proposed ethical frameworks
E. Yaghmaei[15]	2017	Ethical discourse analysis on cybersecurity governance	Highlights accountability and inclusivity in ethics	Lacks empirical grounding	Conceptual orientation without validation
M. S. Jalali and J. P. Kaiser[16]	2018	Systematic review of cybersecurity in healthcare organizations	Frames cybersecurity as a socio-organizational issue	Context-specific to healthcare	Minimal empirical evidence and external validation
V. Švábenský, J. Vykopal, and P. Čeleda[17]	2019	Systematic review of cybersecurity education research (SIGCSE & ITiCSE)	Maps pedagogical trends and educational challenges	Limited dataset scope	Focused only on ACM conference papers
K. Macnish and J. van der Ham[18]	2020	Analytical review of cybersecurity ethics	Clarifies key ethical challenges in cybersecurity research and practice	Relies on conceptual synthesis without empirical testing	Lacks quantitative validation; mainly descriptive conceptualization
J. Pattison[19]	2020	Normative ethical analysis of private cybersecurity interventions	Defines moral boundaries for private cybersecurity defense	Based on philosophical assumptions, not empirical data	Context-specific moral reasoning limits cross-sector applicability
D. Engster [20]	2020	Stakeholder-based ethical framework for business cybersecurity	Integrates care ethics into cybersecurity decision-making	Narrow focus on business ethics	No empirical or industry-based application; conceptual framework only
J. B. Ulven and G. Wangen[21]	2021	Systematic review of cybersecurity risks in higher education	Identifies institutional vulnerabilities and governance needs	Lacks quantitative risk assessment	Limited generalizability beyond higher education
Leitao & Karnouskos [22]	2022	Ethics engineering in cyber-physical systems	Integrates ethics into design	Increases system complexity	Conceptual framework only
D. Kozhuharova, A. Kirov, and Z. Al-Shargabi [23]	2022	Case-based ethical analysis in digital service chains	Identifies major ethical vulnerabilities in cybersecurity ecosystems	Heavy reliance on qualitative interpretation	No data-driven validation or performance metrics provided
R. A. Alsharida et al.[24]	2023	Systematic review of human cybersecurity behavior	Integrates behavioral and ethical dimensions of cybersecurity	Review scope limited to user-centric studies	Does not propose or test a new ethical decision framework
I. Flechais and G. Chalhoub [25]	2023	Mapping CyBOK domains to ethical principles	Links professional knowledge areas to ethical dimensions	Based on workshop and expert opinions only	Small expert sample limits generalizability and reproducibility
S. A. Matei and E. Bertino[26]	2023	Educational framework for AI–cybersecurity ethics training	Promotes ethics and systems thinking in AI security research	Conceptual model; no implementation evidence	Lacks longitudinal validation and pedagogical evaluation
Gupta et al. [27]	2023	Assessment of generative AI in cybersecurity	Highlights dual-use of AI tools	Lacks clear guidelines	Limited ethical frameworks
SciSpace [28]	2023	Survey of key security/privacy papers	Broad coverage of emerging topics	Lacks methodological depth	Descriptive synthesis only
Thirumuruganathan et al. [29]	2024	Bias mitigation in intrusion detection	Reduces sampling bias in IDS	Scalability limitations	Not tested on diverse real-world systems
Damola & Miracle [30]	2024	Algorithmic bias assessment in threat detection	Identifies fairness gaps	High false positives	Narrow dataset scope
Dasu et al. [31]	2024	NeuFair: Dropout-based fairness repair	Improves fairness by 69%	Inference instability	Stochastic behavior affects reproducibility
Mahadik et al. [32]	2024	Privacy-aware IDS for IoMT	Protects patient data	Limited scalability	Tested on narrow medical datasets
MDPI [33]	2024	AI fairness in cybersecurity survey	Comprehensive theoretical overview	Lacks practical application	No evaluation metrics
MDPI [34]	2024	Privacy-aware deep learning IDS	Effective anomaly detection	Complex training procedure	Limited by computational cost

privacy. To preserve health data and address biometric data ethics, micellar-based spectrofluorimetry detection is being used to measure sensitive biomarkers such as cyclic guanosine monophosphate.

Abdelazim et al. (2024) [50] reported that the method accurately and selectively detected cGMP levels in nasal secretions, providing doctors with fresh insights into olfactory dysfunction processes. These technologies are clinically advantageous but also present ethical cybersecurity governance difficulties related to medical data management, distribution, and protection.

Revelation of the NSA's PRISM program has highlighted governments' systematic data collection without authorization or transparency. Such actions violate national

TABLE 2. *(Continued.)* **Comparative summary of ethical cybersecurity.**

GSC Press [35]	2024	Ethics and big data in cybersecurity	Promotes ethical design	Low implementation specificity	Conceptual orientation
CSA [36]	2024	Review of cybersecurity laws 2025	Outlines global legislative changes	Country-level inconsistencies	Implementation lag
P. Ewoh and T. Vartiainen [37]	2024	Systematic review of healthcare cybersecurity ethics	Highlights ethical risks and sociotechnical vulnerabilities	Limited to healthcare context	Context-specific findings cannot be generalized
M. Alanezi and R. M. A. Al-Azzawi [38]	2024	Systematic review of AI-powered cyber threats	Addresses ethical dual-use dilemmas in AI cybersecurity	Theoretical focus; no empirical data	Absence of practical case validation
A. Mubarak and F. Aldhmour [39]	2024	Comparative ethical analysis of hacker ethics and moral hazard	Expands understanding of hacker accountability	Overemphasis on theory	No stakeholder validation or mixed-method evidence
D. Wheeler[40]	2025	Regulatory foresight on privacy and cybersecurity	Highlights ethics-driven, risk-based frameworks and cross-border accountability	Normative projections; lacks empirical testing	Limited validation across diverse jurisdictions and regulatory environments
Kim et al. [41]	2025	Payload-aware IDS using large language models	Improved detection accuracy	Computationally intensive	High resource demands
Berkeley Lab [42]	2025	Geopolitical cybersecurity governance review	Identifies systemic gaps	No global enforcement	Conceptual framework only
M. Mladenov and M. Galetin [43]	2025	Legal-ethical analysis of encryption rights in EU jurisprudence	Establishes encryption as a fundamental right in cybersecurity governance	Focused on European context	Lacks technical or cross-jurisdictional empirical assessment
C. E. Popa Tache and E. N. Vâlcu [44]	2025	Legal–ethical study on AI and corporate liability	Introduces a new ethical-legal contract for AI-driven enterprises	Focused on corporate and legal aspects	Conceptual legal analysis; no applied or industry-level data
This Paper	2025	Integrated ethical framework across cybersecurity tiers	Holistic, valid tier-based ethical integration		Relies on secondary data

constitutions and raise issues about global privacy laws. Experts recommend synchronizing cybersecurity policies with data privacy, fostering openness, and ensuring legal compliance, as well as implementing a unified framework of global cybersecurity standards [6], [7] and [51].

C. CORPORATE RESPONSIBILITY AND DATA BREACH ETHICS

Companies' data breach policies are under closer scrutiny as digital infrastructures become more complex and they retain large volumes of personal data. In the digital economy, organizations must protect and manage sensitive data and information shared by many people. The rising incidence and severity of data breaches suggest that corporations often underestimate the importance of cybersecurity ethics. After a breach, organizations may withhold information from consumers and the public out of fear of legal action, reputation damage, or financial losses, according to Solove and Citron [52] in 2017. People have the ethical right to know if their private information has been compromised, but unreasonable delays prevent this. The authors advocate for strict laws that mandate notice within acceptable timeframes and incident disclosure. Promoting disclosure is an ethical duty in today's more insecure cyber environment, they say. The 2017 Equifax data breach shows how organizational inactivity can violate ethical cybersecurity principles. Equifax overlooked a vulnerability that allowed hackers to access personal data like Social Security numbers, birthdates, and addresses for 147 million Americans. Equifax's month-long delay in revealing the attack compounded the issue when key executives sold company stock just before the event. Equifax's hack management was crucial to corporate ethics talks, showing how poor cybersecurity decisions can have serious ethical and social consequences [53].

Isaak and Hanna (2018) argue that these instances are indicative of a troubling trend in which corporations prioritize cost savings and efficiency before cybersecurity. That strategy may be financially sound, but it poses ethical concerns. Cybersecurity usually becomes a priority after a catastrophe has harmed the public and company. Thus, corporate cybersecurity decisions should consider economic factors, future ethical consequences, resistance to avoidable harm, and community duties [1]. As more activities in almost every facet of daily life rely on digital services, corporations are required to perform a serious moral commitment. In a tech-driven world, entities protect personal data and digital well-being. Martin (2019) and other experts recommend integrating cybersecurity principles into governance procedures, leadership performance indicators, and senior management-monitored policies. Building organizational integrity requires regular security inspections, personnel training, and industry-accepted standards as much as compliance [54].

D. ARTIFICIAL INTELLIGENCE AND ALGORITHMIC ETHICS IN CYBERSECURITY

Academic, government, and industrial experts are increasingly focused on the ethical issues surrounding AI and machine learning in cybersecurity.

Modern cybersecurity occupations use AI for intrusion detection, spam email filtration, user behavior analysis, identity verification, and cyber threat prediction. These technologies offer speed, scalability, and accuracy, but their opaque decision-making processes, lack of transparency, and

risk of harm when unsupervised raise ethical concerns. Due to their inherent opacity, AI systems' findings are difficult to understand, challenging cybersecurity AI ethics. Mittelstadt claims that most deep learning-based AI systems lack transparency.

Developers can barely understand the systems' decisions. Because cybersecurity decisions have real-world effects, the lack of open reasoning raises ethical difficulties. The authors recommend ethical principles that promote transparency, verification, and accountability for end users whenever possible. Recent research shows that machine learning improves IoT cybersecurity sustainability. El Ahmar et al. (2024) [55] showed a multi-algorithmic WSN detection technique that achieved 98% Random Forest, 90% SVM, and 95% KNN detection rates. AI-driven intrusion detection reduces eavesdropping and DoS attacks and enhances authentication and adaptive classification, according to their research.

References [55] and [56] highlight the moral imperative of openness and justice in AI-driven threat detection systems. Algorithmic prejudice creates an ethical dilemma. Historical data-based algorithms tend to reinforce societal preconceptions, such as race, gender, financial class, and geography.

Binns (2018) warns that biased training datasets may cause algorithmic discrimination when AI systems unfairly label poor communities as high-risk or non-compliant without explanation or redress. These assumptions in cybersecurity may unfairly expose certain people or groups to surveillance, inquiry, or restriction of access, aggravating social imbalances and systemic unfairness. Binns recommends incorporating political philosophy and social justice theory into AI governance frameworks to ensure procedural and distributive equity in automated cybersecurity [57].

The ethical governance of AI in cybersecurity raises accountability questions. Who is responsible for an AI system's bad decision? The developer, the company that deployed it, the user who configured it, or the algorithm? The dispersal of responsibility creates a moral vacuum where harm can occur without clear solutions. Jobin et al. (2019) recommend establishing clear responsibility frameworks for AI implementation, including international ethical standards for cybersecurity activities, including human oversight, remedial measures, and post-decision evaluation [58]. The ethical tension between AI system efficiency and human-centered values like privacy, autonomy, and dignity exists. AI-driven behavioral monitoring tools can detect abnormalities and insider threats, but they may invade privacy by tracking user activity, keystrokes, and biometrics.

Despite their potential to increase system security, such surveillance approaches may violate ethics without express authorization and protection safeguards [59].

III. ETHICAL CASE STUDIES ANALYSIS

Cybersecurity ethics analysis is greatly improved by case studies. When these elements interact in disturbing and sometimes harmful ways, cybersecurity ethical dilemmas become clearer. The ethical concerns of famous instances are discussed: Real-world situations have raised ethical issues such as privacy, responsibility, governance, operational resilience, and human rights. Which can help explain cybersecurity ethics. Organizations and politicians may strengthen ethical frameworks like the Tiered Ethical Cybersecurity Model (TECM) by studying key cybersecurity incidents' issues, consequences, and lessons.

Cases were chosen through a deliberate, theory-driven methodology to guarantee their relevance to cybersecurity incidents with quantifiable effects on infrastructure, governance significance, and ethics. The selection criteria were technological background, temporal relevance (2010-2025), and the availability of comprehensive empirical or descriptive data, for thorough cross-case comparison. Each instance was evaluated for benefits, drawbacks, and ethical implications, ensuring that the sample collectively exemplifies significant patterns and enriches both explanatory and normative studies in cybersecurity governance research.

A. CASE STUDIES

1) CASE STUDY 1: STUXNET CYBERWEAPON (2010)

The 2010 discovery of Stuxnet, a complex state-sponsored cyber weapon, is one of the most significant ethical events in cybersecurity. The US and Israel may have secretly developed Stuxnet. Malware was used to disrupt Siemens industrial control systems and hide Iran's nuclear program from observation. Stuxnet was the first cyberattack to harm physical infrastructure, demonstrating a growing foundation for cyberwarfare ethics [60]. Stuxnet delayed Iran's nuclear development with military success but also generated ethical issues. Stuxnet's main concern is the malware's accidental spread to India, Indonesia, and Russia. Despite its inadvertent spread, Stuxnet violates the just war philosophy's ethical standards of non-maleficence and proportionality. Stuxnet was precise, but it lacked sufficient controls to prevent it from affecting unforeseen systems and civilian infrastructures. Cyber warfare ethical concerns include the clandestine attack and reluctance to take responsibility. No country has admitted to using Stuxnet, and cyber warfare lacks legal structures, so victims cannot sue. Buchanan (2020) and Kello (2022) caution that nations' covert cyber hostilities are undermining international order and diminishing accountability and proportionality. Establishing universal cyberspace rules and mediation entities to reduce conflict escalation and destabilization is crucial [61] and [62]. The recent NATO Strategic Concept emphasizes cyberattacks' importance and possible severity for collective defense. The growing use of cyberweapons in combat raises ethical issues. Their ability to supply a tactical edge in battle and cause severe, lasting harm heightens the issue. Stuxnet illustrates how advanced technology and ethics collide. It emphasizes the need for international ethical regulations to regulate cyberattacks'

legal and moral consequences. Military strength, not ethics, may rule cyberspace without such principles [63].

2) CASE STUDY 2: EQUIFAX BREACH (2017, SETTLEMENT 2019)

The 2017 Equifax data breach is one of the most detrimental consumer data breaches in history, affecting the personal information of almost 147 million consumers. The incident transpired because the corporation neglected to implement a patch for a recognized vulnerability in Apache Struts, despite prior warnings some months earlier where the ethical ramifications are extensive, focusing on negligence, accountability, and the obligation of care. Equifax not only neglected to safeguard sensitive information but also postponed public notification, undermining trust and exhibiting a deficiency in openness. In 2019, a deal was achieved providing restitution; nevertheless, many contended that the amount was insufficient considering the extent of the damage, therefore the case highlights the ethical imperative for proactive patch management, stringent internal controls, and restricted preservation of user data. Entities responsible for personal information must serve as custodians, reconciling commercial interests with the inherent right to privacy [63], [64], [65], [66], [67], [68].

3) CASE STUDY 3: FACEBOOK AND CAMBRIDGE ANALYTICA (2018)

Cambridge Analytica improperly obtained data from approximately 87 million Facebook users without their consent in 2018. Users who registered gave the app access to their friends' Facebook profiles. The analysis of data led to the creation of targeted voter influence strategies that impacted the US and UK elections. The incident highlighted serious data privacy and autonomy abuses. Facebook's actions violate its ethical obligation to defend user autonomy and inform personal data decisions. Facebook's response emphasizes corporate transparency and accountability challenges. Experts say the company's poor monitoring processes, algorithmic filter bubbles, and failures encouraged targeted political messages [1] and [90].

Platform operations require serious ethical inquiries. The privacy and security of user data are crucial for Facebook. Facebook was motivated by user-generated data revenue, which led to unethical behavior. To explain cybersecurity's ethical complexity, ethical regulatory frameworks must emphasize users' rights, decency, and democracy.

4) CASE STUDY 4: SOLARWINDS SUPPLY-CHAIN COMPROMISE (2020–2021)

SolarWinds exposed flaws in the global software supply chain. Several clients, including U.S. government agencies and multinational businesses, received Orion IT monitoring platform updates with malicious code. It took months to identify the stealth compromise, raising ethical problems about vendor accountability and software process integrity. Despite issuing advisories, the extended dwell time enabled attackers to pilfer crucial data and undermine trust. The case shows software sellers' ethical obligation to protect development environments and regulators' obligation to ensure supply chain transparency. It shows that poor vendor laws can have widespread effects across cultures and jurisdictions, highlighting the ethical dilemma between business confidentiality and public safety [69] and [70].

5) CASE STUDY 5: COLONIAL PIPELINE RANSOMWARE (2021)

Colonial Pipeline, the largest US petroleum pipeline, was shut down by ransomware in May 2021. The disturbance caused East Coast fuel shortages, panic buying, and economic damage. The company had an ethical dilemma: pay the ransom and resume services or decline and prolong public anguish. The culprits received millions in Bitcoin from the Colonial Pipeline, which U.S. authorities seized. Balancing public safety and welfare with inciting criminal behavior was the ethical challenge. The incident also raised questions about critical infrastructure readiness and resilience. To ensure the ongoing provision of vital public services, essential service operators must take extra precautions, create backup plans, and report [71], [72], [73].

6) CASE STUDY 6: NSO PEGASUS SPYWARE (2021)

In 2021, inquiries disclosed the exploitation of Pegasus spyware, created by the NSO Group, to surveil journalists, activists, political leaders, and dissidents globally. Pegasus, first promoted for law enforcement and counterterrorism, was repurposed for monitoring that infringed upon privacy, consent, and essential human rights, so the case underscores the ethical obligation of cybersecurity firms to prevent the misuse of their capabilities for oppressive purposes.

It also underscores the conflict between national security and personal liberties. The Pegasus incident diminished trust in commercial spyware providers and ignited demands for enhanced global regulation of surveillance technologies. The case fundamentally illustrates the ethical necessity of valuing human dignity, openness, and responsibility above profit and political expediency [74].

7) CASE STUDY 7: LOG4SHELL VULNERABILITY (2021)

In December 2021, the Log4Shell vulnerability (CVE-2021-44228) highlighted the systemic risks of open-source software. The Log4j logging framework vulnerability allowed remote code execution on millions of systems, including financial institutions, hospitals, and cloud service providers. Despite timely upgrades, Log4j's heavy use made cleanup difficult, consequently the example shows the ethical tension between exposing vulnerabilities and malicious actors using them. The event also raises questions about volunteer-managed open-source projects used worldwide. Organizations must accept their ethical duty to promote open-source security and manage dependencies. The instance emphasizes

digital ecosystem interdependence and cybersecurity governance shared responsibilities [75] and [76].

8) CASE STUDY 8: UBER 2016 BREACH COVER-UP (LEGAL OUTCOME 2022–2023)

The 2016 Uber breach, which compromised data from 57 million users, became ethically problematic not due to the breach itself, but because of the company's intentional concealment.

Executives obscured the issue by compensating the attackers to erase the data instead of reporting it to regulators and users. Only years later, during judicial processes in 2022–2023, did the veracity become clear, then the obfuscation contravened ethical values of transparency, integrity, and the obligation to safeguard users.

The case exemplifies how corporate culture can prioritize reputation over responsibility, thereby exacerbating harm. The judicial outcomes underscored that regulatory compliance is crucial and that whistleblowers are essential in maintaining ethical standards. Concealing breaches diminishes trust, incurs legal repercussions, and lowers public faith in technological platforms [77] and [78].

9) CASE STUDY 9: MOVEIT EXPLOITATION (2023)

Due to third-party platform vulnerabilities, the 2023 MOVEit data breach caused ethical and operational issues across global digital communities. Cl0p, a ransomware outfit, exploited a zero-day (CVE-2023-34362) vulnerability in MOVEit Transfer, a popular secure file transfer service.

Government agencies, healthcare providers, and financial institutions had their sensitive files hacked. Security vulnerabilities showed ethical weaknesses in affected organizations' reactions. Some firms alerted consumers and regulators immediately, while others waited weeks, violating stakeholders' right to be informed and proactive.

Delays compromised transparency, accountability, and the ethical duty to prevent illness. The incident revealed vendor monitoring issues and antiquated encryption methods that failed to protect critical data. Lewis argues that ripple supply chain breaches, like MOVEit, demonstrate the ethical need for proactive safety, timely breach disclosures, and rigorous third-party audits to prevent significant trust breaches [5], [79] and [80].

10) CASE STUDY 10: 23ANDME CREDENTIAL STUFFING (2023)

The 2024 data breach of 23andMe, a leading direct-to-consumer genetic testing company, highlighted the ethical challenge of collecting and using genomic data for commercial purposes. Through credential stuffing, hackers stole personal genetic information from millions of people and disseminated it on hidden web forums, including ancestry, health concerns, and family ties.

Unlike password or credit card leaks, immutable genetic data breaches present serious ethical questions about authorization, privacy, and bias. Many users were unaware that insurers, employers, or even criminals could target people based on genetics or ethnicity by aggregating and cross-referencing data. As scholars like Zuboff have warned, corporate entities may collect sensitive personal data without consent and turn it into profitable information sources [49].

The 23andMe case shows that the current privacy policy fails to protect genetic data, so the infraction marks the start of a new legal framework that prohibits secondary use of genetic data and requires firms to improve verification procedures to protect user autonomy and dignity. Genomic data is sensitive and affects people, families, and ethnic communities, making the assault unethical. Privacy concerns increased as reports showed uneven impacts on various communities. The event showed the importance of multi-factor authentication (MFA) and privacy-focused genetic data management. Genetic testing corporations must act ethically because data misuse can lead to discrimination and stigma, consequently the exploit shows that sectors managing immutable data must protect user confidence [81] and [82].

11) CASE STUDY 11: OKTA SUPPORT BREACH (2023–2024)

Okta's support system hack in 2023 exposed business clients' authentication data. Okta first underestimated the incident's severity. The company provided thorough postmortems, raising ethical concerns about transparency, trust, and timeliness. Okta's identification and access control services are crucial to digital infrastructure, compounding ethical transgressions. The case shows the need for accurate and timely disclosure, as minimizing accidents can worsen harm and weaken confidence. Technical remediation and communication techniques that satisfy clients' right to know about actual hazards are ethical obligations [83].

12) CASE STUDY 12: CHANGE HEALTHCARE RANSOMWARE (2024)

The 2024 ransomware attack on Change Healthcare, a significant U.S. medical billing system, impacted services across the nation. The episode highlighted ethical concerns related to the convergence of public health and financial coercion. Hospitals postponed claims and payments, which may jeopardize the protected health information of millions of patients. The attack underscored the vulnerability of healthcare infrastructure and its significance to the public. Healthcare providers have substantial ethical responsibilities to safeguard patient data and ensure the continuity of services.

The incident underscores the necessity for government-backed resilience initiatives, collaborations between public and private sectors, and contingency planning within the sector to combat cybercrime and ensure patient safety [84].

13) CASE STUDY 13: BYBIT COLD WALLET HEIST (FEBRUARY 2025)

In February 2025, Bybit, a prominent cryptocurrency exchange, experienced a hack of its cold wallet, undermining

one of the most dependable methods for safeguarding digital assets.

Cold wallets, kept offline to prevent remote access, have consistently been viewed as the highest standard of security. The heist led to monetary losses and eroded trust in the cryptocurrency market. The issue raised ethical concerns around fiduciary obligation, compensation for affected users, and transaction transparency. Users entrust asset custody to exchanges, hence requiring these exchanges to implement multi-tiered protections and maintain proactive transparency. Furthermore, as cryptocurrency assets become increasingly significant, regulators and exchanges must cooperate to provide more stringent controls, balancing innovation with customer safety [85].

14) CASE STUDY 14: AZURE AI PROMPT INJECTION EXPLOIT (JULY 2025)

In early 2025, researchers showcased a novel type of attack against Microsoft Azure OpenAI Services, illustrating how adversaries might manipulate the outputs of large language models (LLMs) embedded in cloud-based business applications using rapid injection. Attackers can develop tailored inputs to compel an AI to provide secret information, generate biased or ambiguous responses, or execute undesired orders within business processes. The exploit demonstrated that advanced AI systems implemented at scale may harbor significant latent risks that are insufficiently understood by both developers and end-users. Mittelstadt [14], [57] and [58] assert that AI decision-making is notably opaque, complicating the determination of accountability for decisions made and the imposition of ethical standards.

The Azure issue exemplifies that a lack of transparency and minimal safeguarding of AI outputs can erode user trust and pose ethical risks, such as the exposure of sensitive information and the dissemination of harmful content. It also highlighted the deficiency of user education, as numerous firms integrating generative AI tools failed to recognize their susceptibility to manipulation.

The ethical considerations of the case underscore the urgent necessity to implement robust monitoring systems, develop explainability mechanisms, and incorporate human safety measures to ensure accountability and mitigate unforeseen consequences when utilizing AI for essential services [86] and [87].

15) CASE STUDY 15: BANK SEPAH CYBERATTACK AND DENIAL (MARCH–JUNE 2025)

From March to June 2025, information emerged regarding cyberattacks aimed at Bank Sepah, a prominent Iranian financial institution. Although unofficial sources reported considerable disruptions, the bank and government minimized or refuted the occurrences, then the method elicited significant ethical concerns around transparency, accountability, and consumer protection. While safeguarding national prestige may have prompted denial, the absence of transparency rendered customers susceptible and misinformed regarding hazards to their financial holdings. Financial institutions affiliated with the state have an ethical obligation to balance national interests with their public responsibilities. Concealing or downplaying breaches may reduce immediate reputational harm but ultimately undermines trust in the financial system, so the example exemplifies the ethical duty of governments and banks to transparently recognize incidents and implement corrective actions, thereby enhancing resilience and public trust [88].

Table 3 presents an overview of selected case studies from the actual world between 2010 and 2024 chronologically. Examples illustrate distinct ethical concerns, ranging from a violation of privacy and informed permission to state-sponsored cyber warfare, misuse of surveillance, and corporate malfeasance. Table 3 chronologically delineates the key aspects of each episode, the advantages gained, the ethical deficiencies noted, and the remedies

proposed to address or mitigate the identified ethical flaws. The comparative research provides a clearer understanding of recurring challenges and emphasizes the need to implement integrated ethical approaches in both corporate and public cybersecurity services.

Table 4 shows how deontological ethics apply to data privacy, how utilitarianism conflicts with surveillance ethics and linking each case to specific ethical principles besides that viewing consequences and practical policy implication which could transform anecdotal examples into systematic evidence.

Kantian (deontological) ethics prioritize obligations, principles, and the respect for individual rights; utilitarian ethics concentrate on optimizing overall societal advantages, frequently necessitating trade-offs; and virtue ethics underscore the character and professional integrity of individuals in cybersecurity.

B. FINDINGS AND DISCUSSION

Comparing 15 major cybersecurity instances reveals commonalities and ethical issues. Stuxnet (2010) demonstrated the potential for cyberweapons to disrupt critical infrastructure, setting a precedent for state-sponsored actions. The Equifax (2017) and Facebook–Cambridge Analytica (2018) data breaches highlighted patch management issues and ambiguous data-sharing procedures, emphasizing corporate data stewardship and informed consent. The supply chain vulnerabilities of SolarWinds (2020–2021) and MOVEit (2023) showed that reliable software upgrades and third-party platforms can allow adversaries to enter systems. These events illustrate the importance of SBOMs, continuing surveillance, and vendor responsibility. The disruption of key infrastructures can cause immediate social and economic harm, as demonstrated by the Colonial Pipeline ransomware attack (2021) and the Change Healthcare incident (2024). Both cases demonstrate the tension between ransom payment options and the ethical duty to maintain vital services. The Log4Shell vulnerability (2021) showed the vulnerabilities of widely used open-source dependencies, while

the 23andMe credential stuffing (2023) showed genomic data's sensitivity and underprivileged groups' increased risks. Uber's concealment of a breach (2016, reported 2022–2023) demonstrated the ethical importance of transparency, quick disclosure, and executive responsibility. The Pegasus spyware (2021) and Bank Sepah breach (2025) showed how geopolitical and surveillance-oriented initiatives weaken government structures, raising human rights and national trust concerns.

Recent occurrences like Bybit's cold wallet theft (2025) and the Azure AI prompt injection vulnerability (2025) show how attack vectors are expanding to include decentralized finance and generative AI frameworks. These emphasize multi-layered defenses, red-teaming, and AI-centric threat modeling. The main conclusion is that companies, governments, and organizations have ethical duties to patch, minimize data, disclose, and safeguard users. The argument implies that ethical frameworks and regulatory oversight must grow with technology defenses. Technological innovation will outpace security solutions without better governance and accountability, perpetuating cycles of abuse and distrust. A comprehensive examination of scholarly literature, case studies, and regulatory frameworks uncovers persistent ethical dilemmas in cybersecurity. These include the declining value of data privacy, the vulnerability of private information to exploitation amid increasing surveillance, insufficient control of automated systems, and the lack of stated ethical standards in remote cyber warfare. These findings show that cybersecurity has much higher ethical standards than previously thought.

1) DATA COMMODIFICATION AND ETHICAL EROSION

Cybersecurity's commercial handling of personal data is an ethical issue. To make money, digital platforms collect lots of personal data. Without consent, the approach objectifies and commodifies users' personal data. The event suggested exploiting user data to influence elections. Different approaches monetized confidential information. Profile data manipulated thoughts and actions, predicted behavior, and endorsed candidates. These practices are troubling because they rely on intrinsic information disparities and undermine personal autonomy, which deontological and human rights frameworks support [34]. Insufficient and confusing permission disclosures make users passive contributors to a profit-maximizing system. Therefore, these methods limit consumers' ability to give informed consent and control their personal data. Poor people sometimes lack the resources or choices to protect themselves from invasive data practices, making privacy more vulnerable. [52] She calls ''surveillance capitalism'' a new economic model in which firms use personal data to predict and influence customer behavior. She claims that the paradigm allows companies to influence public discourse and behavior without external oversight., consequently the economic system contradicts Kantian ethics, which prioritizes persons as ends, with modern values like trust, equality, and dignity. Figure 2 shows cybersecurity data commodification's ethical ramifications.

2) PRIVACY VERSUS NATIONAL SECURITY

The discourse on cybersecurity focuses on reconciling national security imperatives with citizens' privacy rights.

The issue has become more pressing in an era of digital reliance, as governments progressively sanction sophisticated tools to detect and counteract significant cyber threats, violent crimes, and foreign interference. However, implementing these initiatives often engenders substantial ethical and legal dilemmas.

Governments assert that extensive surveillance of online activities and the aggregation and examination of information assist in identifying and preventing the escalating threats of cybercrime and terrorism. The concept is based on utilitarian principles, permitting the limitation of individual freedoms if the societal benefits are above the associated costs, so the justification underpins the NSA's PRISM program and analogous activities occurring in nations like the United Kingdom, China, and Russia. Advocates of such surveillance Cite critical information from credible sources.

From an ethical standpoint, these tactics contravene the principles of proportionality, need, and the assurance of due process. The volume and clandestine nature of collected monitoring can frequently encompass data from folks unrelated to any perilous activity. Solove (2021) argues that the fear of visibility in pervasive surveillance leads individuals to reduce their voice, political engagement, and trust in government [2].

Moreover, individuals cannot readily challenge the collection or use of their data due to a lack of transparency and the absence of a substantive mechanism for redress, accordingly the issue is particularly concerning in nations founded on the ideas of liberty and constitutional governance. The ethical contradiction is evident: the endeavor to protect democracy and national security can ironically undermine the liberties essential to both.

Experts contend that a more efficacious strategy integrates the imperative for safety with essential assurances for individual privacy. These frameworks include regulations on transparency, the formation of oversight panels, the incorporation of court reviews, and the delineation of parameters on the scope and duration of surveillance activities. The GDPR and various rulings by the European Court of Human Rights have established norms that enhance privacy protection while tackling cybersecurity dangers in Europe. Table 5 illustrates the ethical conflicts between privacy and national security.

Figure 3 shows the flowchart for operationalizing accountability, privacy, transparency, fairness, and security in cybersecurity functions like governance, data management, incident response, system design, and defense operation. It shows ethics being integrated into cybersecurity measures, demonstrating the interdependence of ethics and technology in the digital environment. Governance and policy relate to accountability, emphasizing the need for regulatory monitoring, compliance mechanisms, and executive cyber risk

TABLE 3. Ethical assessment of prominent cybersecurity case studies and suggested enhancements.

Case Name	IEEE Re.	Author(s) / Case Date	Publication Year	Advantages	Disadvantages	**Suggestions for Case or Model**
Stuxnet Cyberweapon	[60-64] and [89]	Langner, Symantec, ISIS Report / 2010	2010	First cyberweapon to impact physical infrastructure	Unintended spread, lack of accountability	Develop international cyberwarfare protocols with ethical checks
Facebook-Cambridge Analytica	[1] and [90]	Cho, M. / 2018	2018	Highlighted data misuse and transparency failure	Lack of consent and ethical oversight	Implement real-time data access controls and transparency dashboards
Equifax Breach	[53] and [66]	FTC Report, Equifax / 2017	2019	Settlement compensated consumers; raised public awareness of patching needs	Failure to patch Apache Struts vulnerability; delayed disclosure; inadequate restitution	Enforce strict patch management, minimize sensitive data storage, stronger breach reporting laws
SolarWinds Supply-Chain Compromise 35	[70] and [91]	Perlroth (NYT), US Gov / 2020	2020	Prompt advisories issued; exposed supply-chain risks to policymakers	oversight Delayed identification; degradation of trust	Strengthen vendor security audits, Implement Software Bill of Materials (SBOMs), establish a zero-trust framework, and conduct third-party monitoring, enforce supply-chain transparency
Colonial Pipeline Ransomware	[72] and [92]	DOJ Report / 2021	2021	Partial ransom recovery; emphasized critical infrastructure protection	Major disruption to fuel supply; ransom paid; panic buying	Mandate resilience standards for critical infrastructure, transparency in ransom handling
Log4Shell Vulnerability	[76] And [77]	NVD CVE-2021-44228 / 2021	2021	Rapid disclosure; global collaboration on patches	Global exposure; slow patching in some orgs; systemic risk due to dependency	Invest in dependency management, continuous vulnerability scanning, secure-by-design libraries
NSO Pegasus Spyware 38	[75] and [93]	Amnesty International / 2021	2021	Uncovered misuse of spyware; global awareness of surveillance abuse	Severe privacy violations; targeting of journalists and activists	International regulation of spyware, transparency on lawful use
Uber Breach Cover-Up	[78] And [79]	US v. Uber / 2016 breach, legal outcome 2022–2023	2022–2023	Legal accountability enforced; whistleblowers highlighted	Ethical breach of trust; user data risk concealed	Corporate culture of transparency, stronger penalties for concealment
MOVEit Exploitation	[80] and [81]	Progress Software Advisory / 2023	2023	Prompt vendor advisories; exploited risk awareness	Widespread exploitation; third-party data loss	Stronger vendor monitoring, third-party risk assessment
23andMe Credential Stuffing	[82] And [83]	23andMe Report / 2023	2023	Disclosure of ethnic-targeting impact; raised genetic privacy concerns	Weak authentication; disproportionate risk to minorities	Enforce MFA, adopt privacy-by-design, limit sensitive data exposure
Okta Support Breach	[84]	Okta / 2023	2024	Post-mortem reports improved transparency	Initial underreporting damaged trust	Improve incident response communication, rapid and accurate disclosures
Change Healthcare Ransomware	[85]	HHS Report / 2024	2024	Exposed healthcare cybersecurity gaps; sparked federal resilience efforts	Nationwide billing disruption; patient data risk	Prioritize healthcare cybersecurity as public infrastructure, gov. investment in resilience
Bybit Cold Wallet Heist	[86]	Bybit Exchange / 2025	2025	Prompt freeze of withdrawals; transparency on losses	Major crypto theft; shaken investor trust	Enhance cold wallet isolation, multi-signature protections
Azure AI Prompt Injection (EchoLeak)	[87] and [88]	Aim Labs / MSRC / 2025	2025	Raised awareness of AI-specific attack surfaces	Exfiltration of sensitive data via zero-click prompts	AI red-teaming, prompt filtering, secure AI design principles
Bank Sepah Cyberattack	[89]	Media Reports / 2025	2025	Brought geopolitical cyber risks into spotlight	Service denial, public distrust due to denial of attack	Transparent communication, national-level incident reporting

accountability. As shown by the Uber breach deception and the Equifax fiasco, corporations may downplay security without specific accountability. Data management affects privacy; therefore, companies must ensure permitted gathering, minimum retention, and encryption.

Privacy management failures like Cambridge Analytica and 23andMe credential stuffing show how supervision affects society. Incident response requires transparency because quick disclosure and transparent communication affect post-breach credibility.

Uber's 2016 cover-up damages trust, but open disclosures like those following the MOVEit and SolarWinds breaches build resilience through collective defense. System design should avoid bias, disproportionate harm, and exclusion.

Cybersecurity involves protecting vulnerable groups like poor communities affected by 23andMe genetic data

TABLE 4. Linking ethical cybersecurity Cases with ethical principles (Kantian, Utilitarian, and Virtue Ethics), consequences and policy implication.

Case No.	Ethical Principles			Consequences / Ethical Dilemmas	Policy Implications / Suggestions
	Deontological	Utilitarian	Virtue		
1	Duty to avoid harm	risk-benefit trade-off	professional prudence	Unintended spread; lack of accountability; ethical concerns in offensive cyber operations	Develop international cyberwarfare protocols with ethical checks; ensure accountability
2	Duty of consent & privacy	societal vs. targeted benefits	transparency & honesty	Data misuse; lack of consent; undermined public trust	Implement real-time data access controls; transparency dashboards; enforce consent mechanisms
3	Duty to protect consumer data	trade-offs between convenience and public safety	diligence & foresight	Delayed disclosure; failure to patch; widespread consumer impact	Enforce patch management; minimize sensitive data storage; strengthen breach reporting laws
4	Duty of care to clients	efficiency vs. systemic risk	integrity in vendor management	Delayed identification; trust degradation; supply-chain risk	Strengthen vendor security audits; implement SBOMs; zero-trust framework; third-party monitoring
5	Duty to resist criminals	societal disruption vs. principle	ethical courage	Major fuel supply disruption; ransom paid; public panic	Mandate resilience standards; transparent ransom handling; protect critical infrastructure
6	Privacy duty	security vs. individual rights	ethical judgment	Severe privacy violations; targeting journalists & activists	Regulate spyware; enforce lawful use; ethical guidelines for intelligence tools
7	Duty to prevent harm	societal vs. organizational risk	prudence & responsibility	Global exposure; slow patching; systemic risk	Dependency management; continuous vulnerability scanning; secure-by-design libraries
8	Duty of transparency	reputation vs. societal benefit	honesty	Concealment of data risk; breach of trust	Promote corporate transparency; stronger penalties for concealment
9	Duty of care	rapid advisories vs. exposure	diligence	Third-party data loss; widespread exploitation	Strengthen vendor monitoring; third-party risk assessment; proactive patching
10	Duty to protect sensitive data	security feasibility trade-offs	ethical prudence	Weak authentication; disproportionate impact on minorities	Enforce MFA; adopt privacy-by-design; limit sensitive data exposure
11	Transparency duty	balancing panic vs. trust	responsibility in reporting	Initial underreporting; trust damage	Improve incident response communication; ensure rapid and accurate disclosure
12	Duty to safeguard patient data	service continuity vs. ethical obligation	professional integrity	Nationwide billing disruption; patient data risk	Prioritize healthcare cybersecurity; government investment; strengthen protocols
13	Duty to protect investors	minimizing broader financial harm	accountability	Major crypto theft; shaken investor trust	Enhance cold wallet isolation; multi-signature protections; transparency on losses
14	Duty to secure AI data	security vs. usability trade-off	ethical foresight	Exfiltration via zero-click prompts; AI attack surfaces	AI red-teaming; prompt filtering; secure AI design principles
15	Duty of disclosure	public trust vs. operational secrecy	integrity in crisis response	Service denial; public distrust	Transparent communication; national-level reporting; ethical governance

disclosure. Security and cyber defense are the technical foundation for defending digital infrastructures. Effective defense requires cleanup, surveillance, and ethical foresight in architecture to prevent harm. Attacks from Stuxnet to AI fast injection holes show that security must develop with technology.

Cybersecurity is both technological and ethical, as shown in the graphic. Accountability, privacy, openness, justice, and security improve organizational resilience and public trust.

IV. ETHICAL CYBERSECURITY MODEL (TECM)

In Figure 4 the proposed tiered ethical cybersecurity model (TECM) for every level in cybersecurity has certain ethical aspects that should be discussed in a systematic way in order to provide principled security of the digital infrastructure but before it needs to be validated in next subsection.

The model advances from Technical Architecture; secure coding, bias-aware design, AI transparency to data management; consent mechanisms, privacy-by-design and data minimization which informs operational response; incident ethics review, responsible disclosure and ethical hacking then shaping Organizational Governance; cyber ethics training, compliance monitoring and ethical leadership. These levels ultimately correspond with the Policy Level, where international standards and digital rights rules are formulated.

The TECM model visualizes ethical integration in cybersecurity decision layers and provides a rational, iterative process for assessing ethical impact, responsibility allocation, and policy implications across cybersecurity situations.

A. EMPIRICAL VALIDATION

1) METHODOLOGY

The tiered ethical framework was empirically verified using a rigorous survey method designed to capture perceptions from various stakeholder groups within the cybersecurity profession. The survey measure was intentionally designed to provide both breadth and depth of measurement.

The study comprised three sections: the first collected demographic and background data, including age, gender, job title, and years of experience; the second assessed the framework through Likert-scale items; and the final section included one open-ended question to obtain qualitative

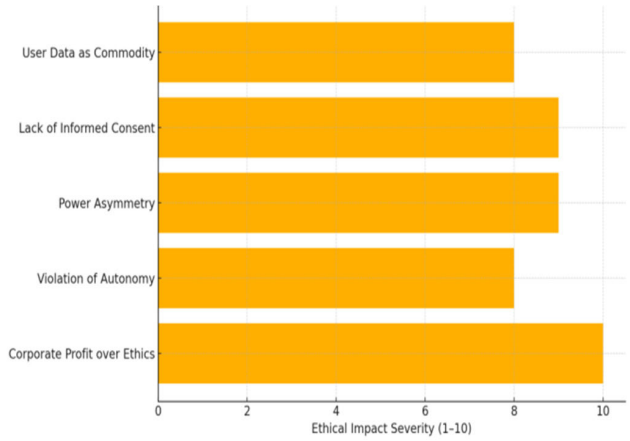


FIGURE 2. Ethical impacts of data commodification in cybersecurity.

feedback on possible enhancements, so the structure facilitated a balance between quantitative accuracy and qualitative depth, enabling a more comprehensive validation of the TECM model.

A total of 500 participants were surveyed, drawn from three primary stakeholder groups: academic faculty, students, and industry professionals. A total of 200 students were recruited from advanced undergraduate and postgraduate programs in computer science, information technology, and cybersecurity. Faculty members (n = 150) were recruited from law, information technology, and applied ethics departments across three universities using purposive sampling to ensure subject-matter competence, therefore the stratified sampling provided balanced representation, facilitating meaningful comparisons among professional roles. Furthermore, participants were located in various countries (Jordan, Saudi Arabia and Malaysia) to examine potential cultural differences in cybersecurity ethics.

A total of 150 professional practitioners from the industry, comprising cybersecurity managers, engineers, and system administrators, were recruited via professional organizations employing a snowball sampling technique. The stratified sample provided a comprehensive representation of attitudes from staff likely to engage with the framework in academic, educational, and practical contexts. The sample size of 500 was adequate to achieve a statistical power exceeding 0.85 for medium effect sizes at a significance level of 0.05, enabling the detection of significant differences.

The opinions of students, teachers, and business professionals from Jordan, Saudi Arabia, and Malaysia were collected by a stratified sampling method. The sample comprised 500 individuals: 200 students enrolled in graduate and undergraduate programs in cybersecurity and computer science, 150 professors from the departments of law, information technology, and applied ethics, and 150 professionals from the cybersecurity sector, including managers, engineers, and system administrators. To ensure subject expertise, teachers were recruited through a targeted procedure, while professionals were identified using a snowball sampling technique incorporating professional networks. A total of around 650 invitations were dispatched, yielding a response rate of 76.9%. For medium effect sizes ($\alpha = 0.05$), the sample size achieved a statistical power above 0.85.

The test was delineated across five primary dimensions: clarity of framework levels (CFT), pragmatic utility (PU), ethical completeness (EC), regulatory fit (RA), and adaptability to new technologies (AT). Each dimension included four statements, resulting in a total of 20 items. The items were evaluated using a 5-point Likert scale, with responses ranging from ''strongly disagree'' (1) to ''strongly agree'' (5), therefore the method generated quantitative data suitable for statistical testing while remaining aligned with the model's theoretical framework. In multidimensional contexts, validation can assess not only the intelligibility of the model but also its perceived relevance, comprehensiveness, and long-term adaptability.

Ethical approval was secured from the Institutional Review Board at Zarqa University (Approval No. ZU-IRB-2025-004). In compliance with institutional and international research ethical standards, all participants provided their informed digital consent prior to the anonymization of their responses, which were thereafter stored in encrypted, access-restricted repositories. All participants granted digital informed permission before engaging, recognizing their voluntary participation, the confidentiality of their responses, and their freedom to withdraw at any moment without repercussions, in compliance with institutional and international research ethics standards.

2) DATA ANALYSIS

Both descriptive and inferential statistical procedures were used in data analysis. To give a summary of the central tendency and dispersion of the data, mean scores, variances, and standard deviations for the various survey dimensions were computed. In terms of mathematics, the standard deviation (s) was calculated by calculating the average response deviation from the mean, and the mean ($\bar{x}$) was obtained by adding up all of the responses and dividing by the total number of participants.

In an attempt to determine the overall distribution of the data, variance was also computed. In order to summarize the respondents' evaluations of the framework across several aspects, basic statistical metrics were essential.

To measure the internal consistency of the survey tool, Cronbach's alpha (α) was calculated for each scale as well as for the entire scale. Cronbach's alpha is a commonly used measure of reliability [94], as follows:

$$\alpha = \frac{k}{k-1}\left(1-\frac{\sum_{i=1}^{k} s_i^2}{s_T^2}\right)$$

where k is the number of items, $\mathbf{s_i^2}$ is the variance of each separate item, and $\mathbf{s_T^2}$ the variability of the total score. Reliability

TABLE 5. Ethical tensions between privacy and national security.

Moral Framework	Utilitarianism: greatest good for the greatest number	Deontology: individual rights must not be violated without due cause
Means of Implementation	Mass surveillance, metadata harvesting, AI-based behavioral analytics	Lack of consent, broad data collection, surveillance of non-suspects
Transparency	Often classified for operational secrecy	Lack of accountability, limited public awareness
Oversight Mechanisms	Executive authority, intelligence agencies	Judicial review, independent watchdogs, legislative scrutiny
Risk of Abuse	Targeted at national threats but can extend to dissent or minorities	Disproportionate targeting, suppression of dissent, erosion of civil trust
Ethical Resolution	Proactive threat detection to ensure public safety	Safeguards, proportionality, and rights-based legal frameworks

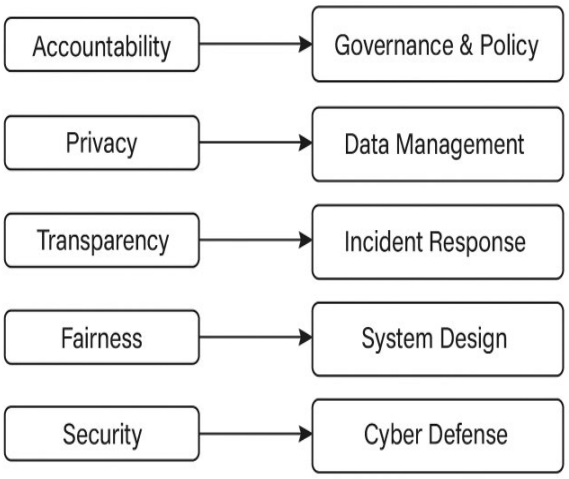


FIGURE 3. Mapping ethical domains to cybersecurity functions.

scores equal to or greater than 0.70 are generally regarded as adequate, with higher scores indicating more consistency.

In a similar manner, inferential statistics were used to investigate group differences. The three stakeholder groups' mean ratings were compared using a one-way Analysis of Variance (ANOVA). Since ANOVA is used to ascertain whether there are statistically significant differences between the means of more than two groups, it is especially suitable for as the kind of analysis. Post-hoc tests (Tukey's HSD) were employed to determine whether groups differed from one another when significant differences were discovered. By comparing observed mean scores to the optimal benchmark of 5.0 for each dimension, gap analysis was also carried out to determine the extent of the framework's evaluation deficiencies.

Besides that, to validate and strengthen the proposed TECM.

Internal consistency was verified using Cronbach's alpha and Composite Reliability (CR) indicating satisfactory reliability. An Exploratory Factor Analysis (EFA) was conducted to investigate the underlying dimensionality of the constructs and the absence of substantial cross-loadings then a Confirmatory Factor Analysis (CFA) was subsequently performed to validate the measurement structure.

Measurement invariance assessments were conducted across several stakeholder groups (academic faculty, students, and industry professionals) and nations ((Jordan, Saudia Arabia and Malaysia) to evaluate cross-context robustness. The findings validated configure, metric, and scalar invariance, hence endorsing the model's generalizability and guaranteeing consistent perception of the constructs across many situations.

3) RESULTS

Descriptive analysis revealed encouraging results. As seen in Table 6, tier clarity registered the highest mean score (M = 4.320, SD = 0.610), revealing respondents were not struggling with understanding the framework and found it well-organized. Pragmatic usefulness was also rated highly (M = 4.110, SD = 0.720), indicating that the participants believe the framework is applicable to the real situation. Ethical completeness was lower (M = 3.890, SD = 0.800), indicating hesitation with whether the framework is addressing all ethical issues in cybersecurity.

Alignment with regulations worked moderately well (M = 4.050, SD = 0.690), suggesting excellent but not flawless alignment with international standards such as GDPR and ISO. Finally, responsiveness to new technologies worked worst (M = 3.760, SD = 0.820), which indicates a critical flaw in the framework's ability to manage rapidly evolving issues such as artificial intelligence, blockchain, and cloud technology, mean and SD shown in figure 5.

Internal reliability of the scale was confirmed through the application of Cronbach's alpha. As evident in Table 7, reliability measures ranged between 0.768 (adaptability) and 0.872 (clarity), with the overall scale at 0.884.

The results indicate excellent internal consistency across the instrument, with none of the dimensions at less than the acceptable 0.70.

Interestingly, aspects such as usefulness and clarity had very high reliability, pointing towards respondents being highly consistent in rating these aspects.

Figure 6 again supports these findings, with all values above the 0.70 criterion for acceptability.

The ANOVA findings in Table 8 confirm statistically significant differences between stakeholder groups. Students ranked clarity most highly (M = 4.410), as would be expected given the value of tiered structure in educational environments.

Faculty members ranked regulatory alignment more strongly than all other groups (M = 4.090), highlighting their focus on legal and normative conformity.

Practical usefulness was considered most important by industry professionals (M = 4.280), indicating their preference for direct applicability.

FIGURE 4. Proposed upward tiered ethical cybersecurity model (TECM).

Industry players, however, were skeptical about ethical completeness (M = 4.010) and flexibility (M = 3.840), their past experiences in rapid-moving technology landscapes wherein models must be adaptable as well as future-proofed.

Gap analysis, as displayed in Table 9, indicated that all the dimensions fell short of the ideal score of 5.0.

The smallest gap was with clarity (0.680), then the largest gap was with adaptability (1.240).

Ethical comprehensiveness (1.110) and regulatory alignment (0.950) were also significantly lacking. Figure 7 provides a visual illustration of the gaps, clearly displaying where the framework must be more precise.

Qualitative feedback gave context to the quantitative results. Open-ended response thematic analysis concluded that three salient themes were: a request for true case studies from the actual world, a need for increased connection to regulatory instruments, and concern for adaptability to domains of nascent technology. Students often noted that although the concept was understandable, it necessitated actual examples to demonstrate its use. The faculty indicated that enhanced compliance with GDPR and ISO standards would enhance its legitimacy.

Industry players emphasized the necessity for adaptability in addressing ethical dilemmas arising from artificial intelligence and blockchain technologies.

Internal consistency was verified using Cronbach's alpha and CR, with all constructs exceeding the recommended threshold, indicating satisfactory reliability, An EFA resulting in robust factor loadings (>0.60). The model displayed satisfactory fit indices (χ^2/df (Chi-square divided by degrees of freedom) = 2.3, CFI (Comparative Fit Index) = 0.95, TLI (Tucker-Lewis Index) also called NNF (Non-normed fit index) = 0.94, RMSEA (Root Mean Square Error of Approximation) = 0.048, SRMR (Standardized Root Mean Square Residual) = 0.041), indicating convergent and discriminant validity all these results shown in tables 10,11, 12 and 13.

4) DISCUSSION

The empirical validation results demonstrate significant evidence regarding the framework's utility and clarity, indicating its usability and accessibility as a guide for ethical decision-making in cybersecurity.

The scale demonstrates high internal reliability ($\alpha = 0.884$), indicating that the survey instrument was clearly articulated and that respondents provided consistent scores across the framework dimensions, accordingly strengthens the validity of the results and supports the argument for employing the framework in educational, academic, and professional settings.

The research identifies a significant area for enhancement. The dimensions of ethical comprehensiveness and flexibility received lower scores compared to others, indicating that although the framework is grounded in fundamental ethical principles, it has not yet fully adapted to the complexities of cybersecurity challenges or the rapid advancement of technology.

This is especially significant in fields like artificial intelligence, block chain, and cloud services, which continually present new ethical challenges. The variation in stakeholder values reinforces the perception that students are straightforward, academics are oriented towards normative fit, and industry professionals are flexible and pragmatic.

The observed differences indicate that the framework should maintain both stability and adaptability, balancing the need for sound ethical guidance with the capacity to address emerging challenges.

5) IMPLICATIONS

The validation has both theoretical and practical implications. The simplicity of the model allows it to function as an educational resource for teaching cybersecurity ethics in lectures, aiding students in organizing their comprehension of ethical values within the online context.

The TECM model offers policymakers a benchmark for aligning with international regulatory standards, ensuring that ethical considerations are integral to cybersecurity policy-making rather than optional.

The TECM model serves as a practical decision-making tool for industry members; however, it requires additional modules tailored for managing new technology.

Incorporating case studies, simulations, exercises, and scenario-based applications within the framework would enhance its utility for all stakeholders.

6) LIMITATIONS

Despite the robustness of these findings, it is important to recognize several limitations.

The research employed a cross-sectional design, capturing perceptions at a specific moment. Therefore, it cannot elaborate on how impressions may change with advancing technologies and ethical dilemmas.

The study employed only three country categories, which restricts the generalizability of cross-cultural comparisons.

Legal and cultural differences significantly influence stakeholders' perceptions of ethical models in cybersecurity.

The reliance on self-reported survey data diminishes confidence in the accuracy of responses concerning practical behavior, particularly in high-stakes cybersecurity contexts.

Subsequent research must address these limitations by implementing longitudinal studies to examine temporal changes in perception, broadening the survey to include participants from multiple nations and cultures, and conducting pilot studies across various companies to test the framework in practical settings.

The study acknowledges numerous limitations, including its cross-sectional design, which restricts causal inference, and the reliance on self-reported measures, which may be susceptible to perception and recollection bias. The geographical scope, restricted to participants from Jordan, Saudi Arabia, and Malaysia, may influence the external validity of the results. Future research will seek to address these limitations through longitudinal studies that examine temporal dynamics in cybersecurity ethical behavior and through multi-institutional pilot implementations to empirically assess the effectiveness and adaptability of the proposed framework beyond perceptual evaluations.

B. INTEGRATING ETHICS AT TECM MODEL TIERS

Incorporating ethics into cybersecurity frameworks necessitates a stratified approach that ranges from overarching policy development to detailed technical architecture. Every tier in the TECM model ensures that cybersecurity measures are both technically resilient and ethically soundly integrating ethical concepts at every level, organizations can attain responsibility, equity, and enduring trust within digital ecosystems.

1. Policy Tier At the apex of the structure, policy delineates the normative basis for ethical cybersecurity.

International standards, digital rights legislation, and ethical agreements facilitate worldwide coherence, guaranteeing that cybersecurity measures uphold essential human rights.

Regulations at this level incorporate ethics by valuing privacy, freedom of expression, and equitable access to digital resources. Policymakers should incorporate ethical norms into treaties and national cybersecurity programs, highlighting the importance of these principles. Integration Strategies: Incorporating human rights concepts into cybersecurity treaties; promoting international collaboration on cyber ethics; creating ethical oversight organizations to supervise policy execution.

2. Governance of the Organization

Governance converts policies into internal mechanisms that influence organizational culture. Ethical integration necessitates proactive initiatives, including cyber ethics training, compliance oversight, and responsibility among leadership. Governance frameworks must equilibrate technological risk management with ethical responsibility, guaranteeing that security decisions include equity and transparency. Ethical leadership is essential, exemplifying integrity and fostering an environment conducive to whistleblowers and ethical conduct. Integration Strategies: Compulsory cyber ethics training for personnel; establishing ethics boards or committees within organizations; incorporating openness and accountability into governance structures.

TABLE 6. Mean and standard deviation of framework dimensions (n = 500).

Dimension	Mean (out of 5)	Standard Deviation
Clarity of Framework Tiers (CFT)	4.320	0.610
Practical Usefulness (PU)	4.110	0.720
Ethical Comprehensiveness (EC)	3.890	0.800
Regulatory Alignment (RA)	4.050	0.690
Adaptability to Emerging Technologies (AT)	3.760	0.820

3. Operational Response

Operational response denotes the organization's immediate activities during security issues. Incorporating ethics necessitates reconciling prompt actions with equity and openness. The ethics evaluation of incidents guarantees that emergency decisions, such as system shutdowns or breach disclosures, prioritize security alongside stakeholder confidence. Responsible disclosure frameworks promote the ethical management of vulnerabilities, reconciling transparency with harm mitigation. Practices of ethical hacking, consistent with. Integration Strategies: Implementing post-incident ethical evaluations; implementing responsible disclosure protocols with explicit timetables; endorsing ethical hacking initiatives such as bug bounty programs.

4. Data Administration

Ethics in data management pertains to the manner in which corporations manage personal and sensitive information. The rapid expansion of big data and artificial intelligence necessitates ethical integration to maintain confidence.

Consent mechanisms must transcend intricate legal terminology to guarantee informed and substantive consent for users. Privacy-by-design concepts integrate ethical considerations into system design, establishing user rights as a fundamental component rather than a secondary concern. Data reduction guarantees that only essential information is collected and retained. Integration Strategies: Developing intuitive permission methods; incorporating privacy-by-design principles into all systems; implementing data minimization to mitigate unnecessary risk exposure.

5. Technical Architecture

The technical layer supports the overall TECM model, guaranteeing that ethical ideals are included in system design and execution. Secure coding approaches incorporate ethics by averting negligence that may result in harm. Bias-aware algorithms promote equity in automated decision-making, tackling issues of discrimination in AI systems.

Transparency in artificial intelligence, exemplified via explainable AI models, fosters responsibility and cultivates user trust. Ethical technical design encompasses accessibility, guaranteeing systems.

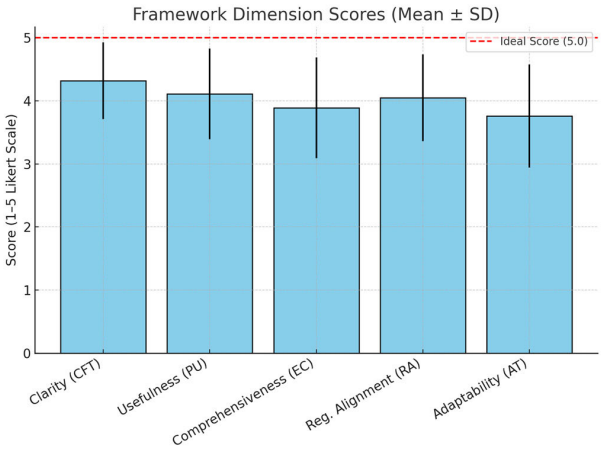


FIGURE 5. TECM dimension ratings (mean ± standard deviation) based on Likert scale responses (n = 500).

TABLE 7. Cronbach's alpha reliability scores.

Dimension	Items	Cronbach's α	Interpretation
CFT	4	0.872	Good
PU	4	0.861	Good
EC	4	0.789	Acceptable
RA	4	0.804	Good
AT	4	0.768	Acceptable
Total Scale (20 items)	20	**0.884**	Good

TABLE 8. ANOVA outcomes across stakeholder groups.

Dimension	Students (n=200)	Faculty (n=150)	Industry (n=150)	F	p-value
CFT	4.410	4.200	4.350	4.22	0.016*
PU	4.010	4.120	4.280	5.01	0.008*
EC	3.710	3.950	4.010	3.67	0.026*
RA	3.950	4.090	4.110	2.94	0.052
AT	3.600	3.850	3.840	4.88	0.009*

Integration Strategies: Using secure coding practices checked by ethical reviews; creating algorithms that recognize bias and promote fairmindedness; ensuring that AI in decision-making tools is clear and understandable.

Cross-Tier Reinforcement:

Although each tier serves a unique function, ethical principles must permeate all tiers to maintain coherence. For instance, rules at the highest-level dictate organizational governance, which then influences operational responses and technical implementations.

Data management decisions must correspond with organizational governance and overarching policy guidelines. Ongoing training, ethical audits, and leadership responsibility function as reinforcing mechanisms at all levels, ensuring that ethics stays integral.

1) TECM IN COMPARISON TO ETHICAL AI FRAMEWORKS

Although NIST [95], EU AI Principles [96], and OECD [97] standard frameworks prioritize risk management, human-centric values, and policy guidance, they continue to be predominantly fragmented or based on principles. The TECM model enhances these approaches by presenting an integrated, context-aware evaluative framework that links ethical traceability, regulatory coherence, and adaptive decision-making mechanisms. The comparative shown in table 14.

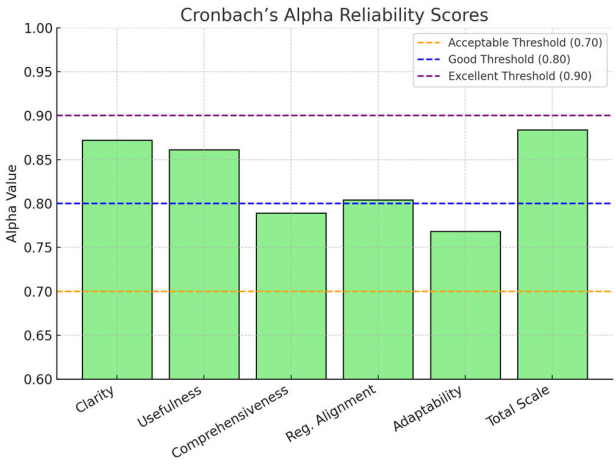


FIGURE 6. Cronbach's alpha reliability.

TABLE 9. Gap analysis of TECM model dimensions.

Dimension	Ideal Score (5.000)	Observed Mean	Gap	Interpretation
CFT	5.000	4.320	0.680	Clear, minor refinement needed
PU	5.000	4.110	0.890	Integration of practical cases required
EC	5.000	3.890	1.110	Broader ethical coverage needed
RA	5.000	4.050	0.950	Strong alignment but not global
AT	5.000	3.760	1.240	Largest gap; urgent updates for AI & blockchain

Final Assessment

The TECM model illustrates the systematic integration of ethics into cybersecurity procedures, from policy formulation to technical architecture.

Each level necessitates unique ethical techniques; nonetheless, they are interrelated, together constituting a comprehensive ethical framework. By integrating ethics at every level, firms go from reactive compliance to proactive responsibility, protecting individual rights and public faith in digital systems.

V. FINDINGS AND DISCUSSION

The study investigated the intersection of cybersecurity with sophisticated technology and the intricacies of interconnected networks in the contemporary world. Cybersecurity is identified in the analysis as both a technological concern and an ethical need.

The research indicates that issues such as data monetization, pervasive surveillance of individuals, insufficient openness in AI systems, and interstate wars conducted in

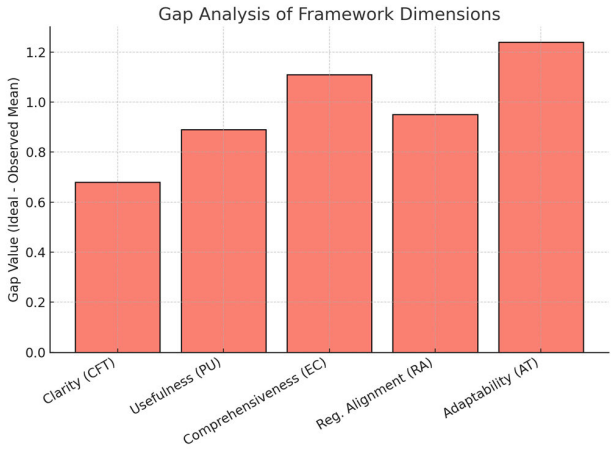


FIGURE 7. Gap analysis.

TABLE 10. Validity and reliability measures.

Construct	No. of Items	Cronbach's α	Composite Reliability (CR)	Average Variance Extracted (AVE)
Technical Architecture (TA)	3	0.876	0.892	0.62
Data Management (DM)	3	0.881	0.894	0.65
Operational Response (OR)	3	0.888	0.903	0.68
Organizational Governance (OG)	3	0.890	0.911	0.67
Policy Level (PL)	3	0.885	0.901	0.64
Average	—	0.884	0.900	0.65

cyberspace pose significant ethical dilemmas. Instances of ignorant consent, reduced personal autonomy, absence of unambiguous responsibility, and heightened risks of significant harm due to inadequate ethical oversight are among the potential dangers. Neglecting cybersecurity ethics in critical infrastructure and operations heightens the potential of committing significant breaches of democracy and internationally safeguarded rights.

However, the uniform implementation of ethical standards in relation to evolving technology continues to fall short of the advancement of norms and regulations. A worldwide accord, enforceable rules, and cooperative measures across nations are essential to effectively address and alleviate the ethically concerning impacts of modern technology and digital surveillance in business.

Cybersecurity ethics encompasses not only the restriction of access to advanced technology but also the assurance that its utilization adheres to the principles of justice, fairness, transparency, and human rights.

In light of the findings and ethical analysis provided, the following recommendations are put forth for governments, corporations, and cybersecurity professionals:

- Ethics must be incorporated at every stage of the development and implementation of cybersecurity systems, encompassing code design and the creation of training data. It necessitates performing comprehensive effect assessments, engaging pertinent parties, and completing multi-faceted ethical reviews.
- Cybersecurity legislation must be complemented by enforceable ethical principles that protect against risks that undermine human rights. Agencies tasked with computer and internet security should possess the authority to assess and scrutinize security activities and to investigate any occurrences of misbehavior.
- Companies must ensure that consumers may offer informed, voluntary, and unambiguous consent for the utilization of their data. Individuals should possess the capability to oversee and alter the utilization of their personal data in real time, retaining the right to decline or delete digital records pertaining to themselves.
- Global governments must collaborate on a treaty that restricts the circumstances under which states may initiate offensive cyberattacks. The agreement must adhere to principles of proportionality, protect people from excessive harm, encourage public condemnation of cyberattacks, and mandate reparations for victims of such actions.

TABLE 11. Factor load (EFA).

Construct (Items)	Item Code	Standardized Loading	t-value	Sig. (p)
TA: Secure coding, AI transparency	TA1–TA3	0.71–0.84	11.25–14.02	<0.001
DM: Privacy-by-design, consent mechanisms	DM1–DM3	0.73–0.86	10.98–13.64	<0.001
OR: Incident ethics review, disclosure	OR1–OR3	0.75–0.88	12.31–14.10	<0.001
OG: Leadership, compliance, ethics training	OG1–OG3	0.72–0.87	11.48–13.95	<0.001
PL: International norms, digital rights laws	PL1–PL3	0.74–0.85	12.06–13.77	<0.001

TABLE 12. Model fit indices (CFA).

Fit Index	Recommended Threshold	Model Value	Interpretation
χ^2/df	< 3.00	2.31	Acceptable fit
CFI	≥ 0.90	0.95	Good fit
TLI	≥ 0.90	0.94	Good fit
RMSEA	≤ 0.06	0.048	Good fit
SRMR	≤ 0.08	0.041	Excellent fit

TABLE 13. Invariance measurements across group.

Invariance Type	χ^2 Δ	df Δ	CFI Δ	RMSEA Δ	Invariance Achieved
Configural	—	—	—	—	Yes
Metric	14.52	10	0.002	0.001	Yes
Scalar	19.87	12	0.004	0.002	Yes
Strict	21.35	14	0.006	0.003	Yes

- Ethics must be an integral component of the training and qualifications for cybersecurity professionals. Comprehending the ramifications of their acts, alongside the statutes and principles regulating cybersecurity, must constitute a fundamental component of the skills imparted to them.
- All societal stakeholders must collaborate to guarantee the ethical administration of cybersecurity procedures. Various players in the cybersecurity domain must collaborate to establish cyber rules and maintain mutual accountability through the transparent exchange of information.

VI. RECOMMENDATION

Based on the ethical analysis, case studies, examination of recent research and the valid ECM model many recommendations are presented:

1. Governments and multinational organizations must prioritize the development of legally enforceable mechanisms to delineate acceptable conduct in cyberspace. Such agreements must include regulations regarding offensive cyber operations targeting civilian infrastructure, standards of proportionality for state-sponsored cyberattacks, and mechanisms for accountability in transboundary attacks.
2. Enterprises engaged in essential digital services and the preservation of sensitive information should mandate the establishment of real-time breach notification protocols. Explicit guidelines about the timing and content of disclosures may aid in safeguarding users' rights to access information and in the collective management of incidents.
3. Institutions must adopt ethical AI frameworks that encompass transparency, explainability, and fairness, particularly as AI systems penetrate increasingly sensitive domains of cybersecurity, so the entails the dissemination of model documentation, robust validation procedures to detect bias, and significant human oversight of the automation's decisions.
4. All the case studies underscore the urgent need to implement rigorous vendor risk assessments and contractual requirements. Organizations must conduct regular security audits to ensure that third-party partners comply with ethical and technological standards and adhere to best practices.
5. Cybersecurity workers should undergo formal training in applied ethics, relevant legislation, and human rights codes. Certification programs and ongoing education should incorporate modules on ethical decision-making, privacy protection, and the societal ramifications of cybersecurity technology.
6. Companies handling personal or sensitive data must establish clear and accessible privacy policies and channels. A framework of methods such as TECM model must be established to empower users to manage the collection, sharing, or deletion of their data while respecting their sovereignty and dignity.
7. To instill public confidence in cybersecurity practices, independent oversight authorities must be established to evaluate these policies, investigate breaches, and impose sanctions for any unethical conduct. These institutions should operate transparently and include academia, civil society, and the commercial sector.
8. Functioning TECM model as an educational resource for teaching cybersecurity ethics.
9. TECM model can be used as policymakers a benchmark for aligning with international regulatory standards.
10. TECM model with other modules serves as a practical decision-making tool for industry members
11. Incorporating case studies, simulations, exercises, and scenario-based applications within TECM model would enhance its utility for all stakeholders.
12. Finally, Organizations can utilize organized instruments such as ethical risk assessment checklists, evaluative tools, and key performance indicators (KPIs) to monitor compliance with privacy, fairness, and security norms.

These recommendations can be summarized as:

TABLE 14. TECM in comparison to ethical AI frameworks.

Framework	Core Focus	Key Principles / Components	Limitations	Distinct Contribution of TECM
NIST AI Risk Management Framework (2023)	Risk identification and mitigation	Trustworthiness, transparency, accountability	Primarily technical and risk-centric; limited ethical adaptability	TECM extends NIST by embedding *ethical traceability* and adaptive evaluation within socio-technical contexts.
EU AI Principles (2021)	Human-centered and lawful AI	Human agency, transparency, safety, non-discrimination	High-level principles with limited operationalization mechanisms	TECM operationalizes these principles through measurable ethical indicators and contextual governance layers.
OECD AI Principles (2019)	International policy coordination and accountability	Inclusive growth, fairness, transparency, robustness	Policy-oriented; limited evaluative and adaptive components	TECM complements OECD by providing a *dynamic, evaluative model* bridging policy intent and applied governance.
TECM (This Study)	Integrated ethical governance and model evaluation	Ethical traceability, contextual adaptability, cross-regulatory alignment	–	Offers a unified evaluative framework integrating ethics, compliance, and adaptive governance across jurisdictions.

- Educational Integration: TECM can help cybersecurity students understand how technology, company policies, and ethics interact in real life.
- Policy Benchmarking: TECM can help policymakers ensure ethical cybersecurity principles for national and organizational cybersecurity to ensures ethical and technical decisions.
- Organizational Risk Assessment: TECM can identify IT system ethical issues for helping them allocate cybersecurity resources to minimize user and stakeholder harm.
- Decision-Support Tool: TECM helps management and cybersecurity teams make ethical decisions when technological solutions violate user privacy or societal standards.
- Incident Response Planning: TECM can map ethical dependencies across layers to better incident response strategies to guarantees technical corrections and ethical accountability in answers.
- Software and technology design: TECM principles can assist developers build in privacy, fairness, and openness before the technology is used, preventing ethical issues.
- Benchmark for Ethical Audits: TECM standardizes IT system ethical audits, helping companies comply with the law and society.

VII. CONCLUSION, FUTURE WORK AND EXECUTIVE SUMMARY

The article asserts that cybersecurity transcends mere technicality; it possesses a moral dimension that necessitates the intentional integration of ethical principles into system design, governance, and operations. A comprehensive examination of contemporary literature on the subject, alongside an analysis of notable case studies including Stuxnet, SolarWinds, MOVEit, 23andMe, Azure AI and more concerning the challenge of prompt injection, has enabled the paper to address the persistent issues of transparency, proportionality, informed consent, and accountability.

The proposed tiered ethical framework (TECM) would emphasize the necessity of embedding ethics inside the technical, organizational, and regulatory dimensions to bolster resilience and trust in digital ecosystems.

Notwithstanding the study's contribution to the comprehensive understanding of cybersecurity ethics, certain deficiencies remain; the swiftly advancing landscape of emerging technologies, such as quantum computing, generative AI, and extensive surveillance, is poised to present new ethical challenges that surpass the parameters of the analysis.

A future pilot study utilizing the TECM model can enhance the investigation of the applicability of ethical frameworks across various operational contexts.

Longitudinal research assessing the efficacy of ethical interventions on organizational behavior, user trust, and regulatory compliance would have substantial importance for policymakers and practitioners alike. Furthermore, it is imperative to build interdisciplinary collaboration among ethicists, engineers, legal scholars, and industry stakeholders to design adaptive governance models that can respond to evolving dangers while safeguarding fundamental rights. Integrating TECM into workflows such as design reviews, procurement, and staff training guarantees that ethical practices are embedded within technical, organizational, and policy levels.

Ultimately, fostering an ethical culture in cybersecurity necessitates not only technical safeguards and regulatory compliance but also a collective appreciation for human dignity, justice, and stewardship of the digital ecosystem.

A. EXECUTIVE SUMMARY

Given the growing ethical quandaries inside today's digital infrastructure, the accompanying essay will provide a practical guide on how to codify ethical concerns as part of cyberspace security initiatives. It presents a valid tiered ethical cybersecurity model (TECM) in which major ethical principles such as accountability, fairness, transparency, privacy, and respect for human dignity are assigned to practical cybersecurity operations such as data governance, incident response, technical architecture, organizational control, and policy development. The framework will serve as a valuable model for decision-makers in both the public and private sectors as they seek to integrate ethics into system design, worker behaviors, and cross-border data processing. It will enable businesses to take a proactive approach to researching the ethical consequences of their digital behaviors by providing training, governance, and open communication.

ACKNOWLEDGMENT

The authors would like to thank Zarqa University for their knowledge and insight, which were very advantageous to the research.

DATA AVAILABILITY

Data is available based on personal request.

COMPETING INTERESTS

There are no competing interests among the authors.

AUTHOR CONTRIBUTIONS

Each author has contributed as shown in the figure below.

Authors Name	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Jafar Ababneh	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Majed Alnemari		✓		✓	✓	✓			✓	✓	✓	✓		✓
Hani Attar	✓	✓			✓	✓	✓		✓	✓	✓		✓	✓
Hani A. Alghamdi	✓	✓		✓	✓				✓	✓	✓			
Muath Al-Shawaheen					✓	✓	✓			✓	✓	✓		
Balqies Saqarat					✓	✓		✓		✓	✓	✓		
Laila Abu Romma					✓	✓			✓	✓	✓		✓	
Musab IQtait			✓	✓	✓		✓		✓	✓	✓			
Mohamed Hafez				✓	✓	✓				✓	✓		✓	

C : Conceptualization
M : Methodology
So : Software
Va : Validation
Fo : Formal analysis
I : Investigation
R : Resources
D : Data Curation
O : Writing - Original Draft
E : Writing - Review & Editing
Vi : Visualization
Su : Supervision
P : Project administration
Fu : Funding acquisition

REFERENCES

[1] J. Isaak and M. J. Hanna, "User data privacy: Facebook, Cambridge analytica, and privacy protection," *Computer*, vol. 51, no. 8, pp. 56–59, Aug. 2018, doi: 10.1109/MC.2018.3191268.

[2] D. J. Solove, "The myth of the privacy paradox," *George Washington Law Rev.*, vol. 89, no. 1, pp. 1–51, Jan. 2021.
[3] L. Floridi and M. Taddeo, "The ethics of information warfare," *Minds Mach.*, vol. 24, no. 4, pp. 331–337, Nov. 2014, doi: 10.1007/s11023-014-9351-9.
[4] D. Lyon, *The Culture of Surveillance: Watching as a Way of Life*. Cambridge, U.K.: Cambridge Univ. Press, 2018.
[5] J. A. Lewis, "The hidden costs of cyberattack," CSIS, Washington, DC, USA, Tech. Rep., 2021. [Online]. Available: https://www.csis.org/analysis/hidden-costs-cyberattack
[6] NIST. (Jul. 2018). *Framework for Improving Critical Infrastructure Cybersecurity*. [Online]. Available: https://www.nist.gov/cyberframework
[7] *Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53 Rev. 5*, NIST, Gaithersburg, MD, USA, Sep. 2020.
[8] L. Floridi, "Translating principles into practices of digital ethics: Five risks of being unethical," *Philos. Technol.*, vol. 32, no. 2, pp. 185–193, 2019, doi: 10.1007/s13347-019-00354-x.
[9] N. H. A. Rahim, S. Hamid, M. L. M. Kiah, S. Shamshirband, and S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness," *Kybernetes*, vol. 44, no. 4, pp. 606–622, Apr. 2015.
[10] P. K. Kushwaha, V. Bibhu, B. P. Lohani, and D. Singh, "Review on information security, laws, and ethical issues with online financial systems," in *Proc. Int. Conf. Innov. Challenges Cyber Secur.*, Noida, India, Feb. 2016, pp. 79–83, doi: 10.1109/ICICCS.2016.7542301.
[11] N. Kumar, N. Kharkwal, R. Kohli, and S. Choudhary, "Ethical aspects and future of artificial intelligence," in *Proc. Int. Conf. Innov. Challenges Cyber Secur. (ICICCS-INBUSH)*, Noida, India, Feb. 2016, pp. 111–114, doi: 10.1109/ICICCS.2016.7542339.
[12] D. Kavallieros, C. Chalanouli, G. Kokkinis, A. Panathanasiou, E. Lissaris, G. Leventakis, G. Giataganas, and G. Germanos, "Searching for crime on the web: Legal and ethical perspectives," in *Proc. Int. Conf. Cyber Secur. Protection Digit. Services (Cyber Security)*, Glasgow, U.K., Jun. 2018, pp. 1–8, doi: 10.1109/CyberSecPODS.2018.8560689.
[13] A. Wilk, "Cyber security education and law," in *Proc. IEEE Int. Conf. Softw. Sci., Technol. Eng. (SWSTE)*, Herzliya, Israel, Jun. 2016, pp. 94–103, doi: 10.1109/SWSTE.2016.21.
[14] B. Mittelstadt, "Ethics of the health-related Internet of Things: A narrative review," in *Proc. Ethics Inf. Technol.*, vol. 19, Sep. 2017, pp. 157–175, doi: 10.1007/s10676-017-9426-4.
[15] E. Yaghmaei, "Cybersecurity and ethics: A white paper on the ethical discourse in cyber-security," SSRN Preprint, Social Sci. Res. Netw. (SSRN), Rochester, NY, USA, 2017.
[16] M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: A systematic, organizational perspective," *J. Med. Internet Res.*, vol. 20, no. 5, May 2018, Art. no. e10059, doi: 10.2196/10059.
[17] V. Švábenský, J. Vykopal, and P. Čeleda, "What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE conferences," 2019, *arXiv:1911.11675*.
[18] K. Macnish and J. van der Ham, "Ethics in cybersecurity research and practice," *Technol. Soc.*, vol. 63, Nov. 2020, Art. no. 101382.
[19] J. Pattison, "From defence to offence: The ethics of private cybersecurity," *Eur. J. Int. Secur.*, vol. 5, no. 2, pp. 233–254, May 2020.
[20] D. Engster, "A care-based stakeholder approach to ethics of cybersecurity in business," in *The Ethics of Cybersecurity*, M. Christen, B. Gordijn, and M. Loi, Eds., Cham, Switzerland: Springer, 2020, pp. 119–138.
[21] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2, p. 39, Feb. 2021, doi: 10.3390/fi13020039.
[22] P. Leitao and S. Karnouskos, "The emergence of ethics engineering in industrial cyber-physical systems," in *Proc. IEEE 5th Int. Conf. Ind. Cyber-Phys. Syst. (ICPS)*, May 2022, pp. 1–8, doi: 10.1109/ICPS51978.2022.9816931.
[23] D. Kozhuharova, A. Kirov, and Z. Al-Shargabi, "Ethics in cybersecurity: Challenges and handling approaches," in *Cybersecurity of Digital Service Chains*. Cham, Switzerland: Springer, 2022.
[24] R. A. Alsharida, B. A. S. Al-Rimy, M. Al-Emran, and A. Zainal, "A systematic review of multi perspectives on human cybersecurity behavior," *Technol. Soc.*, vol. 73, May 2023, Art. no. 102258.
[25] I. Flechais and G. Chalhoub, "Practical cybersecurity ethics: Mapping CyBOK to ethical concerns," in *Proc. New Secur. Paradigms Workshop*, Segovia, Spain, Sep. 2023, pp. 62–75.
[26] S. A. Matei and E. Bertino, "Educating for AI cybersecurity work and research: Ethics, systems thinking, and communication requirements," 2023, *arXiv:2311.04326*.
[27] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "Tunable quantum criticality in multicomponent Rydberg arrays," 2023, *arXiv:2308.12838*.
[28] SciSpace. (2023). *Top 71 Security and Privacy Papers Published in 2023*. Accessed: Aug. 2025. [Online]. Available: https://typeset.io/
[29] S. Thirumuruganathan, "Detecting and mitigating sampling bias in cybersecurity," in *Proc. USENIX Secur. Symp.*, Apr. 2024, pp. 1–18.
[30] P. Damola and A. Miracle, "Effect of AI algorithm bias on the accuracy of cybersecurity threat detection," ResearchGate, Berlin, Germany, Dec. 2024. [Online]. Available: https://www.researchgate.net/
[31] V. A. Dasu, A. Kumar, S. Tizpaz-Niari, and G. Tan, "NeuFair: Neural network fairness repair with dropout," 2024, *arXiv:2407.04268*.
[32] S. S. Mahadik, P. M. Pawar, R. Muthalagu, N. R. Prasad, S.-K. Hawkins, D. Stripelis, S. Rao, P. Ejim, and B. Hecht, "Digital privacy in healthcare: State-of-the-art and future vision," *IEEE Access*, vol. 12, pp. 84273–84291, 2024.
[33] M. Lataifeh, N. Ahmed, S. Elbardawil, and S. Gordani, "Assessing the legibility of Arabic road signage using eye gazing and cognitive loading metrics," *Computers*, vol. 13, no. 5, p. 123, May 2024, doi: 10.3390/computers13050123.
[34] MDPI. (2023). *Current Trends in AI and ML for Cybersecurity: A State of the Art Survey*. Accessed: Aug. 2025. [Online]. Available: https://www.tandfonline.com/
[35] L. K. Nwobodo, C. S. Nwaimo, and A. E. Adegbola, "Enhancing cybersecurity protocols in the era of big data," *GSC Adv. Res. Rev.*, vol. 19, no. 3, pp. 203–214, 2024, doi: 10.30574/gscarr.2024.19.3.0211.
[36] "Global cloud security regulations and compliance report 2025," Cloud Security Alliance, Seattle, WA, USA, CSA Rep., Nov. 2024.
[37] P. Ewoh and T. Vartiainen, "Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review," *J. Med. Internet Res.*, vol. 26, May 2024, Art. no. e46904.
[38] M. Alanezi and R. M. A. Al-Azzawi, "AI-powered cyber threats: A systematic review," *Mesopotamian J. CyberSecurity*, vol. 4, no. 3, pp. 166–188, Dec. 2024.
[39] A. Mubarak and F. Aldhmour, "Cybersecurity ethics and ethical hackers: A systematic overview on data availability and moral hazard in cyberspace," in *Artificial Intelligence, Digitalization and Regulation: A Legal Framework for Business*. Cham, Switzerland: Springer, 2024.
[40] D. Wheeler, "Privacy and cybersecurity regulatory expectations for 2025," Harvard Law School Cybersecurity Project, Cambridge, MA, USA, Tech. Rep., 2025.
[41] Y. Kim, C. Lee, and Y. Yoon, "Payload-aware intrusion detection with CMAE and large language models," 2025, *arXiv:2503.20798*.
[42] *Reflections on Cybersecurity Futures 2025: Looking Back From the Present*, Berkeley Lab, Berkeley, CA, USA, May 2025.
[43] M. Mladenov and M. Galetin, "The unbreakable code shaping digital resistance: A right to encryption in the jurisprudence of the European court of human rights and the court of justice of the European union," *Juridical Tribune-Rev. Comparative Int. Law*, vol. 15, no. 3, pp. 578–591, Oct. 2025.
[44] C. E. Popa Tache and E. N. Valcu, "Artificial intelligence and corporate liability towards a new legal-ethical contract in the dynamics of emerging global human rights convergences," *Juridical Tribune-Rev. Comparative Int. Law*, vol. 15, no. 2, pp. 281–305, Jun. 2025.
[45] J. Ababneh, A. Abu-Jassar, S. Abuowaida, V. Liubchenko, and V. Lyashenko, "Evaluation of three different operators for object highlighting in medical RGB images: Canny, roberts, and LoG in independent color spaces," in *Proc. 25th Int. Arab Conf. Inf. Technol. (ACIT)*, Zarqa, Jordan, 2024, pp. 1–7, doi: 10.1109/ACIT62805.2024.10876948.
[46] M. Manjikian, *Cybersecurity Ethics: An Introduction*. Evanston, IL, USA: Routledge, 2017.
[47] B. C. Stahl, I. J. Timmermans, and E. Flick, "Ethics of emerging information and communication technologies: On the implementation of responsible research and innovation," *Sci. Public Policy*, vol. 43, no. 3, pp. 369–381, 2016, doi: 10.1093/scipol/scv082.
[48] P. A. E. Brey, "Anticipating ethical issues in emerging IT," *Ethics Inf. Technol.*, vol. 14, no. 4, pp. 305–317, Dec. 2012, doi: 10.1007/s10676-012-9293-y.
[49] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY, USA: PublicAffairs, 2019.

[50] M. H. Abdelazim, F. Alsenani, A. Alharbi, F. H. Baali, A. H. Baali, M. H. Abduljabbar, R. M. Alnemari, and M. A. Algarni, "Spectrofluorimetric determination of cyclic guanosine monophosphate in human nasal secretions: Evaluating levels in healthy individuals and patients with olfactory dysfunction," *BMC Chem.*, vol. 19, no. 1, p. 171, Jun. 2025, doi: 10.1186/s13065-025-01530-1.

[51] *General Data Protection Regulation (GDPR)*, Official Journal of the European Union, Brussels, Belgium, Apr. 2016.

[52] D. J. Solove and D. K. Citron, "Risk and anxiety: A theory of data-breach harms," *Tex. Law Rev.*, vol. 96, no. 4, pp. 737–786, Mar. 2018.

[53] EPIC. *The 2017 Equifax Breach*. Accessed: Sep. 6, 2025. [Online]. Available: https://archive.epic.org/privacy/data-breach/equifax/

[54] K. E. Martin, "Designing ethical algorithms," *MIS Q. Exec.*, vol. 18, no. 2, pp. 129–143, Jun. 2019, doi: 10.2139/ssrn.3565193.

[55] E. E. Ahmar, A. Rachini, and H. Attar, "Cybersecurity enhancement in IoT wireless sensor networks using machine learning," *WSEAS Trans. Inf. Sci. Appl.*, vol. 21, no. 1, pp. 480–487, Oct. 2024.

[56] G. Dodig-Crnkovic, "Floridi's information ethics as macro-ethics and info-computational agent-based models," in *Luciano Floridi's Philosophy of Technology: Critical Reflections*. Dordrecht, The Netherlands: Springer, 2012, pp. 3–22, doi: 10.1007/978-94-007-4292-5_1.

[57] R. Binns, "Fairness in machine learning: Lessons from political philosophy," in *Proc. Conf. Fairness, Accountability Transparency*, Apr. 2018, pp. 1–11, doi: 10.1145/3287560.3287582.

[58] A. Jobin, M. Ienca, and E. Vayena, "The global landscape of AI ethics guidelines," *Nature Mach. Intell.*, vol. 1, no. 9, pp. 389–399, Sep. 2019, doi: 10.1038/s42256-019-0088-2.

[59] B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, and L. Floridi, "The ethics of algorithms: Mapping the debate," *Big Data Soc.*, vol. 3, no. 2, Dec. 2016, Art. no. 2053951716679679, doi: 10.1177/2053951716679679.

[60] P. Singer, "Stuxnet and its hidden lessons on the ethics of cyberweapons," *Case West. Reserve J. Int. Law*, vol. 47, no. 3, pp. 79–86, 2015.

[61] B. Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA, USA: Harvard Univ. Press, 2020.

[62] L. Kello, *Striking Back: The End of Peace in Cyberspace-and How to Restore It*. New Haven, CT, USA: Yale Univ. Press, 2022.

[63] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy*, vol. 9, no. 3, pp. 49–51, May 2011, doi: 10.1109/MSP.2011.67.

[64] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier," Symantec Corporation, Mountain View, CA, USA, Tech. Rep., Feb. 2011. [Online]. Available: https://www.symantec.com

[65] *Committee on Oversight and Government Reform, The Equifax Data Breach*, U.S. House Representatives, Washington, DC, USA, Dec. 2018. [Online]. Available: https://oversight.house.gov

[66] Apache Software Foundation. (Mar. 2017). *Apache Struts Security Vulnerability Alert: CVE-2017-5638*. [Online]. Available: https://struts.apache.org/security

[67] L. Ablon, "Consumer data breaches and the responsibility to protect personal information," *Commun. ACM*, vol. 63, no. 11, pp. 18–20, Nov. 2020, doi: 10.1145/3383441.

[68] FTC. (Jul. 22, 2019). *Equifax to Pay $575 Million as Part of Settlement*. [Online]. Available: https://www.ftc.go

[69] S. S. Alqahtani, A. Alzahrani, and A. A. Alqarni, "SolarWinds supply chain attack: Analysis, implications, and lessons learned for cybersecurity governance," *IEEE Access*, vol. 10, pp. 79232–79248, Jul. 2022, doi: 10.1109/ACCESS.2022.3196637.

[70] S. U. Khan, A. Hakak, W. W. Ahmed, and M. Imran, "Cybersecurity risks in software supply chains: A post SolarWinds analysis and future research directions," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Rhodes, Greece, Apr. 2022, pp. 223–230, doi: 10.1109/CSR54599.2022.9850326.

[71] *Colonial Pipeline Ransomware Attack*, U.S. Department of Justice (DOJ), Washington, DC, USA, 2021.

[72] A. Hemsley and L. Jacobs, "Ransomware risk and critical infrastructure protection: Lessons from colonial pipeline," *J. Cyber Policy*, vol. 7, no. 2, pp. 259–278, 2022, doi: 10.1080/23738871.2022.2082090.

[73] P. J. Polack, M. Newhouse, and N. Carter, "Ransomware and critical infrastructure: Lessons from colonial pipeline," *J. Cybersecurity*, vol. 8, no. 1, pp. 1–13, Jul. 2022, doi: 10.1093/cybsec/tyac012.

[74] B. Marczak, J. Scott-Railton, L. McKune, N. Selvakumar, and R. Deibert, "Pegasus: Corporate surveillance in the digital age," *Int. J. Intell. Counter Intell.*, vol. 36, no. 4, pp. 663–696, Oct. 2023, doi: 10.1080/08850607.2023.2184916.

[75] B. Guo, J. Chen, Y. Xiao, and X. Du, "A comprehensive study of the Log4j vulnerability: Exploitation, detection, and mitigation," *IEEE Access*, vol. 10, pp. 58671–58684, Jun. 2022, doi: 10.1109/ACCESS.2022.3180024.

[76] NIST. (Dec. 2021). *NIST Special Publication: Security Advisory—CVE-2021-44228 (Apache Log4j Remote Code Execution)*. [Online]. Available: https://www.cisa.gov/log4j

[77] "Uber data breach case outcome," Court Proceedings, U.S. District Court, Northern District of California, U.S. V. Uber Technologies, San Francisco, CA, USA, 2023.

[78] *Uber Enters Non-Prosecution Agreement Related to 2016 Data Breach*, U.S. Attorney's Office, San Francisco, CA, USA, 2022.

[79] U. K. A. B. G. Khan, "Analysing the exploitation of MOVEit and MOVEit cloud: Cybersecurity risks, attack vectors, and mitigation strategies," *Int. J. Inf. Technol.*, vol. 4, no. 1, pp. 108–123, Jun. 2023, doi: 10.34218/ijit_04_01_013.

[80] G. Kennedy. (2023). *The-Cl0p-Heist: Data Stolen in the MOVEit Zero-Day Attack-Blitz*. [Online]. Available: https://www.mayerbrown.com/en/insights/publications/2023/06/the-cl0p-heist-data-stolen-in-the-moveit-zero-day-attack-blitz/

[81] R. Holthouse, S. Owens, and S. Bhunia, "The 23andMe data breach: Analyzing credential stuffing attacks, security vulnerabilities, and mitigation strategies," 2025, *arXiv:2502.04303*.

[82] W. J. Buchanan, S. Grierson, and D. Uribe, "Privacy-aware single-nucleotide polymorphisms (SNPs) using bilinear group accumulators in batch mode," 2024, *arXiv:2401.07691*.

[83] D. Bradbury, "Unauthorized access to Okta's support case management system: Root cause and remediation," Okta Security Blog, San Francisco, CA, USA, Tech. Rep. [Online]. Available: https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause

[84] G. P. Kanter, J. R. Rekowski, and J. T. Kannarkat, "Lessons from the change healthcare ransomware attack," *JAMA Health Forum*, vol. 5, no. 9, Sep. 2024, Art. no. e242764, doi: 10.1001/jamahealthforum.2024.2764.

[85] D. S. Krause, "The bybit hack of February 2025: Anatomy of the largest cryptocurrency theft in history," *Int. J. Crypto Curr. Res.*, vol. 5, no. 1, pp. 52–62, 2025.

[86] S. Yoosuf, T. Ali, A. Lekssays, M. AlSabah, and I. Khalil, "StructTransform: A scalable attack surface for safety-aligned large language models," 2025, *arXiv:2502.11853*.

[87] OWASP. (May 2025). *LLM01:2025 Prompt Injection—OWASP Gen AI Security Project*. [Online]. Available: https://genai.owasp.org/llmrisk/llm01-prompt-injection/

[88] A. Davidi, "Cybercrime or political warfare? The 2025 bank-sepah hack and the vulnerability of Iran's financial system," *J. Intell. Strategic Stud.*, vol. 2, no. 1, pp. 27–41, Jun. 2025.

[89] J. A. Lewis, "Stuxnet, revisited (again): Producing the strategic relevance of cyber weapons," *Secur. Stud.*, vol. 10, no. 2, pp. 89–93, 2025, doi: 10.1080/23738871.2025.2492570.

[90] M. Cho, "The Facebook-Cambridge analytica scandal: An analysis of care," M.S. thesis, Dept. Eng. Soc., School Eng. Appl. Sci., Univ. Virginia, Charlottesville, VA, USA, 2024. [Online]. Available: https://libraetd.lib.virginia.edu/downloads/707958958

[91] A. Kruti, U. Butt, and R. B. Sulaiman, "A review of SolarWinds attack on orion platform using persistent threat agents and techniques for gaining unauthorized access," 2023, *arXiv:2308.10294*.

[92] S. Srinivasan and L.-K. Ni, "Ransomware attack at colonial pipeline company (HBS case, nos. 123–069)," Harvard Bus. School, Tech. Rep., 2023.

[93] K. Kareem, "A comprehensive analysis of pegasus spyware and its implications for digital privacy and security," 2024, *arXiv:2404.19677*.

[94] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, Sep. 1951, doi: 10.1007/bf02310555.

[95] *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST, Gaithersburg, MD, USA, 2023.

[96] *Ethics Guidelines for Trustworthy AI, High-Level Expert Group on Artificial Intelligence (AI HLEG)*, European Commission, Brussels, Belgium, 2021.

[97] *Organisation for Economic Co-Operation and Development (OECD), OECD Principles on Artificial Intelligence*, OECD Legal Instruments, Paris, France, 2019.

JAFAR ABABNEH (Member, IEEE) received the B.Sc. degree in telecommunication engineering, in 1991, the M.Sc. degree in 2005, and the Ph.D. degree in 2009. In 2009, he joined as the Head of computer information and network systems in information technology(IT), WISE University, for four years. He was the Dean of the IT faculty, WISE University, for more than five years. In March 2022, he joined the Abdul Aziz Al Ghurair School of Advanced Computing (ASAC), LUMINUS Technical University College (LTUC) for two years. He joined the Cyber Security Department, Faculty of Information Technology, Zarqa University, Jordan, in January 2024. He is an Associate Professor. He has published many research papers, book chapters, patents, and books in international refereed journals and conferences. His research interests include congestion and network performance, wireless and mobile networks, cybersecurity, wireless sensor networks (WSNs), artificial intelligence, data mining and retrieving information, cloud computing, and E-learning.

MAJED MOHAMMED ALNEMARI received the Bachelor of Science degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia, and the M.Sc. degree from Muta university, in 2025. His field of interest was computer science. He now holds the position of Head of the Communications and Information Technology Department. He has extensive professional expertise in information systems administration, secure communications infrastructure, and technology integration within a military context, among other areas. Current study areas include cybersecurity ethics, data privacy, and the cutting-edge use of technology for military reasons.

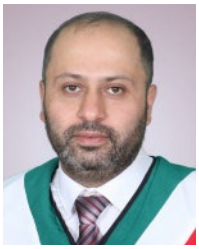
HANI ATTAR received the Ph.D. degree from the Department of Electrical and Electronic Engineering, University of Strathclyde, U.K., in 2011. Since 2011, he has been a Researcher of electrical engineering and energy systems. He is currently the University Lecturer of Zarqa University, Jordan. His research interests include renewable energy systems, efficient designs, and wireless communications.

HANI A. ALGHAMDI is a Senior Systems Development Director with extensive experience leading digital transformation initiatives across government and defense sectors. His professional focus lies in designing and managing secure, mission-critical information systems that support national operations and public services. With a background that combines technical leadership and organizational strategy, he has contributed to the development of integrated platforms for surveillance, threat management, and operational coordination. He has a strong track record of driving innovation, enhancing system reliability, and ensuring alignment with institutional goals under high-security and high-availability requirements. Currently pursuing advanced academic research, his interests center on cybersecurity in critical infrastructures, AI-driven threat detection, and digital evidence acquisition methodologies. His work bridges practical system design with emerging academic insights, contributing to the evolving landscape of secure and adaptive information systems. He has received multiple awards for excellence in government technology and continues to engage in research that supports national resilience and technological advancement.

MUATH AL-SHAWAHEEN received the Bachelor of Science degree in computer science from Mutah University, in 2008. His primary focus was computer science. He possess extensive professional expertise in information system administration, secure communication infrastructure, and technology integration, among other areas. Current study areas include cybersecurity ethics, data privacy, and the cutting-edge use of technology.

BALQIES SAQARAT received the bachelor's degree in computer engineering from Mutah University in 2006, with a solid academic background in both hardware and software systems. She is currently concentrating on advanced security concepts, threat detection, and safe system design. She possess substantial professional expertise in information systems administration, secure communications infrastructure, and technology integration, gained through years of experience in both technical and administrative capacities.

LAILA ABU ROMMAN received the bachelor's degree in computer engineering from Al-Balqa Applied University (Faculty of Engineering Technology), in 2006, with a solid academic background in both hardware and software systems. Her emphasis is on sophisticated security concepts, threat identification, and safe system architecture. She possess substantial professional expertise in information systems administration, secure communications infrastructure, and technology integration, gained through years of engagement in both technical and administrative capacities. Her research interests include cybersecurity ethics, data privacy, and the strategic use of new technologies for military and national security.



MUSAB IQTAIT received the Ph.D. degree in in artificial intelligence from the Faculty of Informatics and Computing, University Sultan Zainal Abidin, Terengganu, Malaysia. He is an Assistant Professor with the Faculty of Information and Technology, Zarqa University, Jordan. His research interests include image/signal processing, biometrics, and pattern recognition.